Complex security problems of the internet of things

Alexander Shiler[1*], and *Elizaveta* Stepanova[1]

[1]Omsk State Transport University (OSTU), 644046, 34 Marksa Street, Omsk, Russia

Abstract: At present, the Internet market of things is constantly expanding; it has covered almost all the most important areas: transport, housing and communal services, industry, agriculture, telecommunications and information technology. In connection with the constant increase in the number of attacks on IoT-devices, the issue of standardization of this technology is quite acute. The features of the of existing solutions and the new proposed Russian NB-Fi standard for IoT are presented in this article from the point of view of information security.

1 Introduction

At present, the Internet market of things is constantly expanding; it has covered almost all the most important areas: transport, housing and communal services, industry, agriculture, telecommunications and information technology. Now, there is no one consolidated standard for IoT (Internet of things), there are about 300 protocols and technologies for IoT. There are many problems in the field of IoT security: from the standardization to basic security rules, such as changing the default password. Until now, many IoT-devices can be hacked by selecting a pair of "login-password", which were set by default and were not changed by the user.

Attacks performed on IoT devices can be classifying according to their purpose:

1. Attacks aimed at causing physical harm to the user

Examples of such attacks may be the car intelligent control system hacking to take it out of control and harm the driver or passenger; the disabling of medical life support equipment; breaking a smart car wash in order to block the owner's exit from the car and others.

2. Attacks aimed at stealing data

Examples of using IoT vulnerabilities to steal personal or corporate data can be the hacking of video cameras, home voice assistants and other devices.

3. Attacks aimed at capturing IOT device control

Such attacks are performed in order to use the attacked device for their own purposes, for example, for sending spam, illegitimate mining of crypto currency (cryptojacking). The attacked device not only becomes an object of exploitation, but it can also serve as an entry point.

4. Attacks aimed at breaking equipment.

Classification of possible attacks on IoT according to its aims shown in Fig. 1.

[*] Corresponding author: shiler_alex@inbox.ru

Over the last 3 years, the number of botnets attacks on the IoT has grown dramatically. One of the largest botnets that caused much damage was Mirai, later appeared Satori and his successor, Reaper. Such large-scale attacks became possible due to the fact, that many users did not change the standard passwords in their devices, not taking into account the need to protect them. In Table.1 shows the most common usernames and passwords that were using during botnet attacks on IoT.

Multiple vulnerabilities were detected in Dlink 850L routers, WIFICAM wireless IP cameras, Vacron network video recorders and other devices.

Old vulnerabilities, such as the vulnerability of CVE-2014-8361 in Realtek devices, as well as the 2012 vulnerability, which allows to detect the configuration of Serial-to-Ethernet converters, including Telnet-password, through a request to port 30718, are not eliminated. This vulnerability directly affects the industrial Internet of things (IIoT) - serial interface converters underlie many systems that allow the operator of industrial equipment to remotely monitor its state, change settings and manage modes Started [1].

The number of vulnerabilities in the IoT grows according to the IoT infrastructure expansion. Numerous attacks prove that this technology is still at the level of formation and the issues of information security here are very acute.

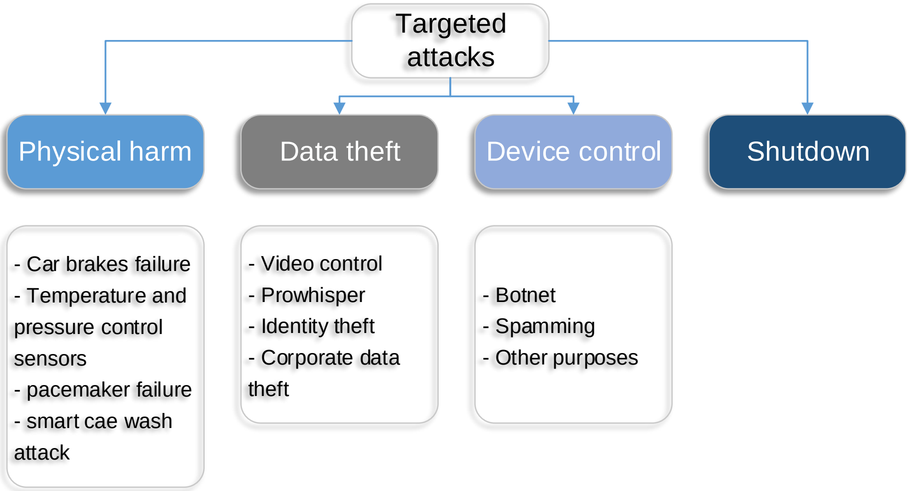

Fig. 1. IoT attack classification

Table 1. Passwords and logins used to attack IoT-devices

Login	Password
root	admin
admin	root
test	1234
access	ubnt
DUP root	123456
DUP admin	password
ubnt	12345
oracle	test
postgres	qwerty
pi	raspberry

2 Communication technology

The concept of the communication for IoT implies providing long-range coverage due to the small amount of periodically transmitted data LPWAN (Low-power Wide-Area Network). The architecture of IoT-networks assumes the existence of a base station (gateway), a server, end devices, in some cases of cloud storage.

There are various technologies for the LPWAN networks, the most popular of which are LoRa, Sigfox and NB-IoT.

LoRa technology introduced in early 2015 by Semtech and IBM Research. LoRa uses the modulation method patented by Semtech, as well as the open network protocol Long Range Wide Area Networks (LoRaWAN), a MAC layer layer (OSI media layer 2) protocol for networks with multiple nodes with a long range and low power consumption. LoRa modulation based on Spread Spectrum Modulation technology and variations of linear frequency modulation (Chirp Spread Spectrum, CSS). Such a solution ensures the stability of communication at large distances. The network can have a different topology: mesh, star, point-to-point, etc. The bandwidth of the signal, recommended for a standard LoRaWAN network, is 125 kHz, which allows organize eight channels of 125 kilohertz [2].

Security in LoRa networks ensured by using two keys based on the block algorithm AES-128: first, the authentication key in the NwkSKey network transmitted, the key for setting up the AppSKey session.

The LoRaWAN protocol provides two methods for authenticating a device on a network:

- using personal settings: occurs by directly recording the network address (DevAddr) issued by the LoRaWAN provider and the NwkSKey and AppSKey encryption keys, either when the device is manufactured, or later, in this case, communication with the server is not required;

- over-the-air activation (using the server): the device sends a request and receives confirmation from the server. The server transmits a unique 32-bit network address, as well as two AES-128 keys.

Over-the-air activation is more reliable, since it allows each time to establish a new session and receive a new key, so you need periodically update the session for each device.

Due to the fact, that the LoRa base stations can determine the packet source only after demodulation, it is possible to block the data transmission channels by sending large number of random data packets. It is also necessary to ensure that each device uses its own unique key, and keep the keys safety.

Currently, there are recommendations for using asymmetric encryption keys for each LoRa device. They are beyond the scope of the standard; however, they must be following for safety. There is a standard NB-IoT (Narrow band IoT), developed by the consortium 3GPP. This is the cellular standard for telemetry devices with low data transmission. In Russia, mobile communication operators are engaged in the promotion of this technology. NB-IoT assumes several scenarios: Standalone, Guard-band, In-band. Standalone - the allowed spectrum is outside the 3GPP UMTS / LTE frequency band. Guard-band - the LTE guard interval is using. In-band - the resources of the allowed spectrum of LTE-frequencies are using, this is one of the most popular deployment scenarios, but it takes away the resources of cellular networks, and also creates mutual interference (Figure 2).

NB-IoT designed to operate in the licensed frequency bands of the uplink channel 890-915 MHz and the downlink 935-960 MHz, the transmitter power is limited to 200 mW, bandwidth – 180 kHz.

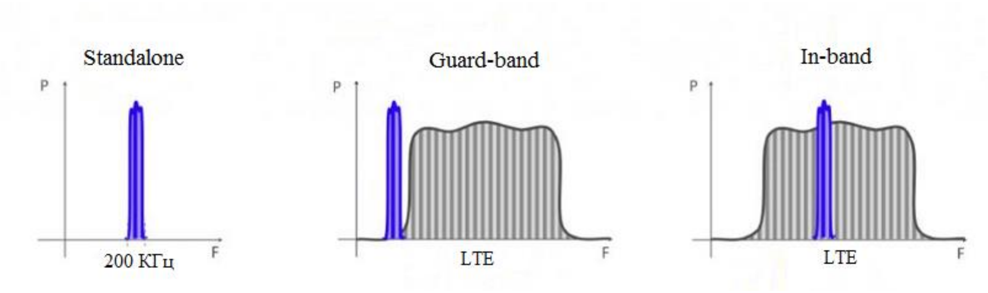

Fig. 2. NB-IoT technology transmission scenarios

Currently, the project of the order of the Ministry of Communications and Mass Communications of the Russian Federation discussing, concerning the implementation of the Russian crypto protection system certified by GOST at the level of sim cards for cell phones.

3 New Russian standard and security

To solve these problems in April 2018, participants of the Russian Association of Internet Things (AIV), established on the initiative of the Internet Initiatives Development Foundation and Bauman MSTU developed a draft national standard protocol NB-Fi of exchange for the Internet of things in the narrow-band spectrum. Now, there is a discussion of the project and everyone can submit their proposals for its completion.

The standard is based on the ultra-narrowband (UNB) phase-manipulated signals, which, in combination with noise-immune coding, allow achieving high sensitivity (up to 150 dBm), whiling the total bandwidth for simultaneous transmission of a large number of channels is sufficient narrow. Network standard NB-Fi, similar to mobile networks, uses the star topology [3]. This standard is based on was the XNB protocol developed by the company "Modern Radio Technologies" ("Strizh"). NB-Fi technology involves the use of a license-free frequency band 868 MHz.

The Strizh network uses its own private Marcato 2.0 protocol and DBPSK differential binary phase shift keying. The protocol provides XTEA encryption using a 256-bit key, the bandwidth of the signal is 100 Hz, which allows organizing 5000 narrowband channels, due to the large number of non-overlapping frequencies, mutual interference between the transmitters not observed. One of the problems with the operation of LPWAN networks is the limitation of bandwidth in the downlink DOWNLINK (from the base station to the terminal devices). It complicates the procedure for remote updating of the "firmware" of devices, when the amount of data transferred increases significantly. To solve this problem, the standard provides using the specialized radio transceivers that allows transmit downlink data by using UPLINK packets, which ensures the transmission of an equal amount of data in the upstream and downstream direction (peer-to- peer). The physical layer of the NB-Fi protocol in this case implemented in the radio transceiver itself.

For encryption, a unique 256-bit key is used. Encryption keys are generating randomly during the file of the license forming procedure on the network operator's server. Each NB-Fi ID is associated with a personal key that is stored on the server and in the output file of the license. The license file is using during the modems firmware procedure. The UPLINK and DOWNLINK data packets contain a field corresponding to the checksum of the unencrypted data. This allows, after decrypting the packet, to verify the reliability of the received data and discard the packet in case of a mismatch between the server keys and the modem [3].

To encrypt data in UPLINK and DOWNLINK packages, a symmetric block code XTEA-256 is using. This is a modification of the outdated TEA code. It is believed that XTEA is well protecting, but you can choose the type of attack for which this code is vulnerable. The most successful attack of all conducted on XTEA is a differential attack on the associated keys, which is able to crack 37 of the 64 rounds of the algorithm, using 263 selected open texts with a time complexity of 2125.

In the preliminary adition of the standard, there are no clear recommendations on encryption of data; there is only an indication that the Payload field can be encrypting with the block code XTEA-2, which leaves the probability of equipment without encryption in order to reduce its cost and overhead for data transmission. There is no information that a modifier with a random content (the so-called "salt") must be added to the hash sum of the password or to the password before hashing to protect against dictionary enumeration.

To ensure reliable delivery of data, you can send packets in the HANDSHAKE_SIMPLE mode. Packets are repeating until the response is receiving or the number of repeated requests is exceed (specified by the program). However, the procedure for signing the packets is not described in any way, the operation of the counter of the sent packets is not described, which leaves the possibility to compromise the system on the channel level by changing the contents of the packet fields or performing a replay attack. To protect against attacks of the "Man-in-the-middle" type, HTTPS / SSL with the RSA algorithm is using.

The issue of protecting the servers themselves, as their logical structure of interaction with the base station and client equipment in the standard is not covered. The issues of secure key storage are also not affected, it is clear that the solution of these problems lies with the user. The question of trust to the operator when storing keys in the cloud is also open.

4 Conclusion

Generally, at present big number of the IoT information security problems shifted to users. The main threat to the Internet of things, remain DDos-attack. In addition to mandatory certification and standardization, it is necessary to develop decisions in the field of responding to incidents of cyberthreats, monitoring IoT networks. To provide information security IoT a comprehensive approach is necessary.

So, let us present the desired architecture of a secure IoT network, which provides a comprehensive approach (Figure 3).

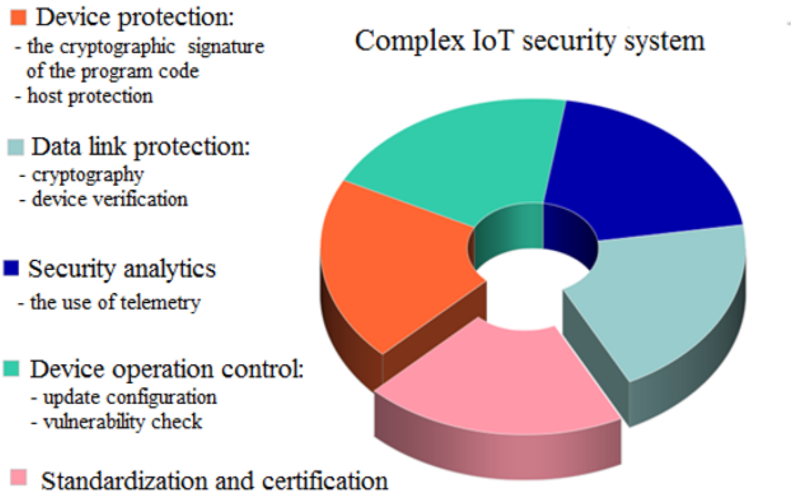

Fig. 3. Complex IoT security model

The presented model consists of:

1. Device protection

Here you need to enable host protection using all necessary procedures: intrusion prevention (IPS, IDS), protection against local attacks (security policy settings, access control), encryption. The security of the hardware directly affected by the security of the code: secure code loading, the use of signed firmware.

2. Security analytics

An integrated approach to security is impossible without using the analytical systems. Analytical security systems can use telemetry from the devices themselves and from network equipment, which will allow you to have up-to-date information about which threats are most relevant. Many IoT networks have certain patterns of behavior, in such systems it is easy to detect deviations.

3. Device operation control

This includes regular checking for vulnerabilities, downloading updates with ready-made fixes for vulnerabilities.

4. Data link protection

When transmitting data over a communication channel, you need to use reliable encryption algorithms. The specificity of IoT-sensors is that a small amount of computing resources does not allow using complex resource-intensive encryption algorithms, however, modern cryptography algorithms, such as, for example, elliptical (ECC) algorithms provides high security level with. When establishing a connection, the authentication procedure of the connected devices is mandatory.

5. Standardization and certification

When building and using any network, it is necessary to follow the accepted standards. As the technology of the Internet of things passes the stage of becoming, the standardization procedure is in process now.

References

1. The landscape of threats to industrial automation systems. Second semester (Kaspersky Lab ISC CERT, 2018)
2. B. Moyer, Electronic engineering journal, September **7** (2015)
3. *Information Technology. Internet of things. Exchange protocol for the Internet of things in the narrow-band spectrum (NB-Fi). Preliminary national standard of the Russian Federation* (Moscow, Standartinform, 2018)