Internet of things is that a threat?

The threat

As we`ve mentioned before, the information security won't be safe and confident without a systematic and comprehensive analysis of all threats.

The new article from PenTestPartners reveals a threat in the internet of things protocol Z_WAVE, which in its turn belongs to the 802.15.4 aka ZigBee standard's family.

This standard runs deeper and deeper into our lives and brings us not only comfort, but also additional risks.

We will not consider merits and demerits of "internet of things" as there is a lot of information about it on the web. We also will not consider the vulnerabilities of these standards the article we`ve mentioned above is just one of them, but we would like to reflect the risk respectively to information leakage channels.

How it works

Let's study the 802.15.4 standard from the RF point of view. Accordingly to the description that can be easily found on the Wikipedia: IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN). The basic framework conceives a 10-meter communications range with a transfer rate of 250 kbit/s. Devices are conceived to interact with each other over a conceptually simple wireless network. Peer-to-peer (or point-to-point) networks can form arbitrary patterns of connections, and their extension is only limited by the distance between each pair of nodes. It operates on one of three possible unlicensed frequency bands:

- 868.0–868.6 MHz: Europe, allows one communication channel (2003, 2006, 2011[4])
- 902–928 MHz: North America, up to ten channels (2003), extended to thirty (2006)
- 2400–2483.5 MHz: worldwide use, up to sixteen channels (2003, 2006)

As we can see frequencies are very similar to worldwide famous standards GSM, Wi-Fi, Bluetooth and this is a real threat, because power of emission of 802.4.15 devices is very low and practically can't be detected with the higher power signal on the background (See figure 1). In common with ability to build self-organized peer-to-peer network this feature allows transmitting intercepted information for the long enough distance to hide a real information receiver.

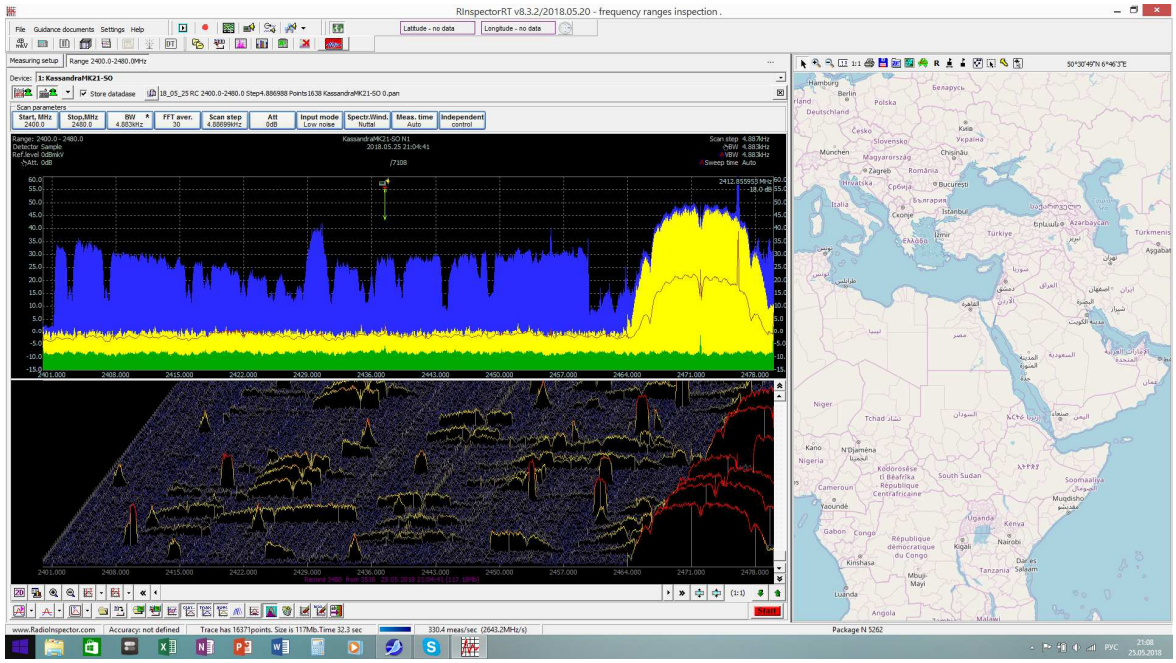

Figure 1. *The frequency of the transmitter is 2430 MHz looks like it below the noise level*

In our practice, we encountered such kind of a problem during our TSCM assistance. A fire alarm detector inside the negotiation room has been changed to a clandestine microphone and eavesdropped information transferred via 802.15.4 network to the voice recorder with the distance near to 150 meters. Later we made some tests in our lab and confirmed transmission of audio information with the quality that allows to understand a human speech pretty clearly.

Our decision

RadioInspector is a unique software product that supports a digital analysis of various digital standards and 802.15.4 standard is included. DTest option is especially developed feature intended to provide a sophisticated digital analysis and automatic demodulation of signal of interest.

We work within a legal spatial and we don't extract information from the packets, but we analyze headers of them and extract addresses and traffic information (See figure 2). The knowledge of addresses of devices and amount of traffic among them allows us to discern legal and illicit devices and suppose what kind of information might be transmitted as well.

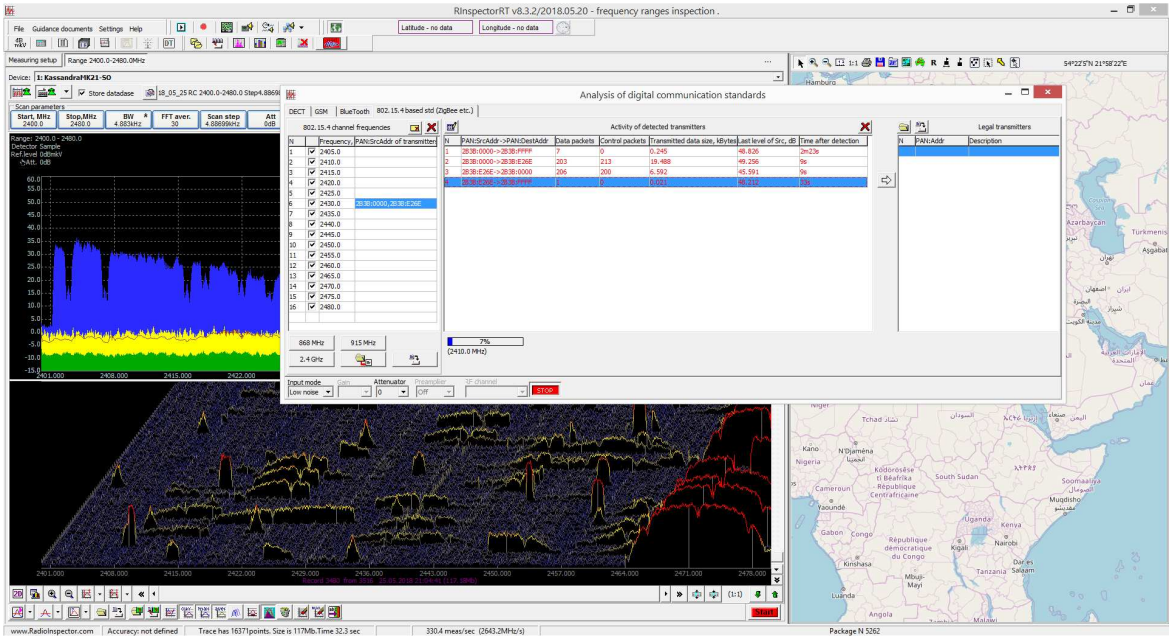

Figure 2. *Information extracted from packet's header allows analysis of the device behavior*

The main evidence that a detected device works in an inappropriate mode is very high traffic, because a speech transmission utilizes bigger amount of the channel's capacity, hence if the quantity of transmitted packets is increasing drastically then we need to inspect device with the appropriate address.

All detected by DTest 802.15.4 devices we can add to the list of legal transmitters and any new device's address appears in red color and should be checked by security staff.

RadioInspector supports more than 200 various spectrum analyzers and SDRs, unfortunately not all of them support IQ stream, but those, which can do it with the bandwidth 5 MHz and more, might be used for the digital analysis of 802.15.4 standard.

The conclusion

Contemporary information security can't be considered as an isolated protection system against threats within logical network data transmission levels from MAC to Application level. A comprehensive analysis of different threats appearing from various spaces only can be a guarantee of information confidence.

The company, which security staff understands that information leakage channels might be on all the levels of the data transmission, will have a very serious competitive advantage.