Developing a Comprehensive Internet Security System

Olexander Belej[1]

1. Department of Computer-Aided Design, Lviv Polytechnic National University, Ukraine, Lviv, Oleksandr.I.Belei@lpnu.ua

Abstract – The article discusses what lies behind the concept of "security of the Internet of Things", and also lists the real problems of the company's customers, which relate to aspects such as hardware and embedded or server software. Solutions that ensure the security of the "Internet of Things" are presented in the same vein as we represent its development over the next years, until our world fully switches to the IPv6 and 6LoWPAN protocols.

Keywords – Internet of Things, security, protocols, software, traffic, security system.

Introduction

Internet of Things (IoT) should be the technology that will help solve many problems facing each of us individually and to humanity as a whole, from the automation of life and ending with the protection of the environment from environmental disasters.

We can appreciate the many benefits of the "open world" today - the Internet allows us to share information, receive education, make purchases, meet other countries, communicate with loved ones and enjoy works of art without leaving our apartment. The Internet blurs the boundaries - national, geographical, cultural, communication - and from this point of view is an absolute good, as it ensures the interaction of all structures of society.

On the other hand, universal internetization has become a favorable environment for the commission of crimes that occur in cyberspace, but, thanks to the same openness, have consequences for the real life of both an individual and whole states. We are talking about the theft of personal data, hacker attacks, hacking servers of national committees and ministries [1].

The same applies to the Internet of things, which is nothing but one of the stages of the development of the world wide web. IoT becomes the union of physical and digital reality, the transformation of the Internet into a "network of networks", which includes all the objects of the surrounding world - not only familiar devices, but also objects that would not seem to be created for the role of "Internet nodes": coffee makers and refrigerators traffic lights and outdoor video cameras, water meters and plumbing devices, medical and industrial equipment [2].

In a general sense, IOT is a set of digital devices that communicate with each other and work autonomously, without human intervention. This is quite enough to reflect on the threats that the transformation of objects into Internet sites brings. And I must say that expert studies of IoT security problems were not long in coming - already in 2008, the "network of networks" appears in the report of the US National Intelligence Council as one of six potentially destructive technologies [3].

7 years later, in early 2015, the OpenDNS company presented disappointing results of a study conducted in corporate networks that use "Internet things". By the way, the OpenDNS brand belongs to Cisco, the world leader in the field of information technology, which, in particular, is associated with the generally accepted wording of the term "Internet of Things" and popularize this phenomenon in general [4].

There are also more recent data - at the beginning of this year, the authoritative online magazine TechRepublic predicted an increase in the number of cybercrimes due to the deplorable state of the "network of networks" security system. Experts have identified several criteria that can lead to real chaos in the infrastructure of the Internet of Things. Here are the main ones:

A fast-growing IoT device park. Today, about 6,000,000 new “things” are online every day! If we consider that each device has not one “hole” in the security system, but several, then the situation is really awesome [5].

Weak security of huge arrays of user data. We add that for correct operation, many IoT devices collect not only passwords, but also information of a different type, starting from the user's name and ending with facts from the biography. Obviously, where a multitude of interrelated data is stored, reliable protection is also required. The Internet of Things cannot boast of it yet.

The ability to quickly create a powerful botnet of millions of devices connected to each other. Before the advent of IoT, this problem was not so acute, which is primarily due to the loss of “autonomy” of the physical world — with the advent of the Internet of Things, “Internet things” no longer work by themselves, but integrated into a single communication structure [6].

Obviously, the security problems of the Internet of Things require an immediate search for solutions, which confirms our review. And the experts' fears, unfortunately, are justified - IoT in its modern form provides great opportunities for the activity of cybercriminals. We give only three real examples.

To enhance the security of IoT, many solutions are offered, but most of them can be summarized as follows:

First, a unified standardization is required, which will establish regulations for each of the areas of the Internet of things. The first step to this has already been taken - in October 2016, information appeared about the plans of the European Commission for the mandatory certification of physical objects of the world integrated into the IoT. Details of this program yet, but as one of the options called the need for chipping "things" connected to the global network. In the context of IoT, we are talking about those devices that in themselves are of no value to criminals, but can be used for hacker attacks and other criminal activities - refrigerators, televisions, video cameras, printers [7].

Secondly, it is necessary to move away from “cross-platform”, which today is one of the main criteria not only for the Internet of Things, but also for the digital reality in general. In other words, each category of devices built into the “network of networks” must come to the use of two or three platforms, no more. For example, all washing machines should be equipped with microcontrollers with typical, rather than different, firmware, video cards should use the same drivers ... While this seems fantastic, but hardware manufacturers, operating system developers, and suppliers should work in this direction [8].

And, thirdly, you need to pay attention to the performance of the software itself. This concerns not only the need to “patch holes” in the efficiency of the applications used, but also the improvement of their scalability, which is especially important given the continuity of the process of incorporating new and new devices into IoT [9].

In conclusion, I would like to say that IoT is only at the beginning of its development, and it would be naive to believe that obstacles and obstacles will not arise in this way. One of these is the vulnerability of the Internet of Things. Despite the complexity of the situation, we have good reasons for optimism - this problem concerns not only the expert community, but also political institutions, commercial structures, and ordinary consumers.

So, together, we will bring a qualitatively new era in the development of the information space. The era of the safe Internet of things.

Regardless of the scope and the protection scheme used, there always comes a time when a device that is connected to another device or a remote server needs someone to store unique identifiers or access keys into the device's memory. This is called device personalization. And it carries with it certain difficulties, which always have to be solved either by the manufacturer of the equipment or by its end user (Fig. 1).

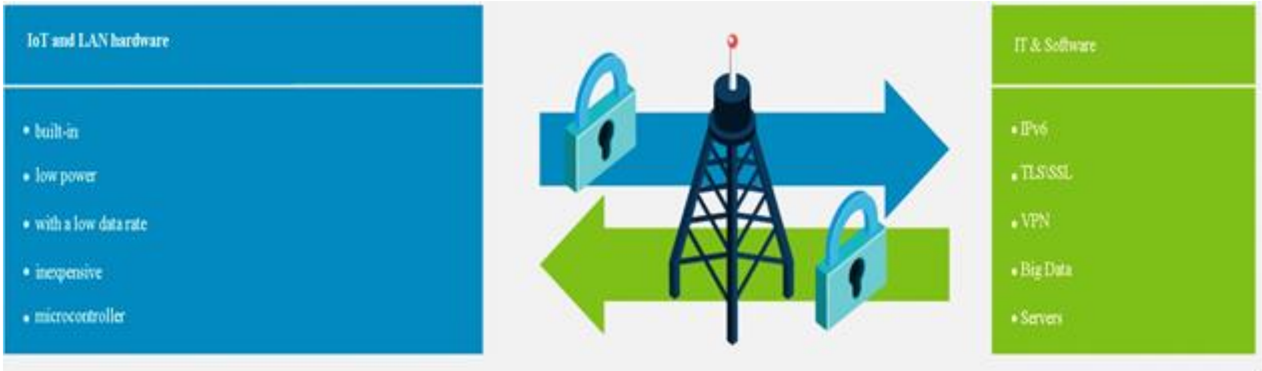


Fig.1. Personalization of devices for the manufacturer and end user

For clarification, we give a simple illustrative example, namely, connecting a Wi-Fi printer to a home network. At some point in order for network users to use the same access key, you will need to manually connect the printer to a Wi-Fi router. It doesn't matter if you'll do this with a wireless connection or via a USB cable, but you'll need to enter a key in the printer In this case, you decide the personalization task, as an end user, not a manufacturer of the printer.

In all these cases, someone has to bear the costs of solving the problem of personalization and the connection process, whether it is a device manufacturer, service provider or end user with their own experience in connecting ready-to-use equipment.

The complexity of these processes often makes them a weak link in network security. How often do you update your access key to your home Wi-Fi network? Perhaps never, since it is too troublesome. The AES-key is updated in our numerous systems not too often, and even never, and for the same reasons.

Channel and network security is currently provided by various communication and network technologies at various levels, sets of protocols, such as IPsec for IP, WPA 802.11, 802.15.4, Bluetooth, and so on? However, they should not be considered as a means to ensure comprehensive end-to-end connection safety. Indeed, having a WPA-secured Wi-Fi connection on a local router is certainly not enough to provide a private HTTP connection on a remote server, since the keys of most local networks are hardly ever updated for the reasons listed above.

The following is a typical situation where data from a sensor or an actuator, before reaching the server you need, is transmitted through many networks of different types owned by a large number of service providers (Fig. 2).

At each link of the transmission, the security of this particular area is ensured by protocols, and what happens before or after it is not known, this is a "secret under seven seals." As a result, the data is decrypted and encrypted again by the security gateways at each site. As you know, the security level of the entire system is determined by the security level of the weakest link. Therefore, the situation with integrated security depends on the security provided by several providers and manufacturers of gateways, and remains entirely on their conscience, which is the weak link of the entire security system.

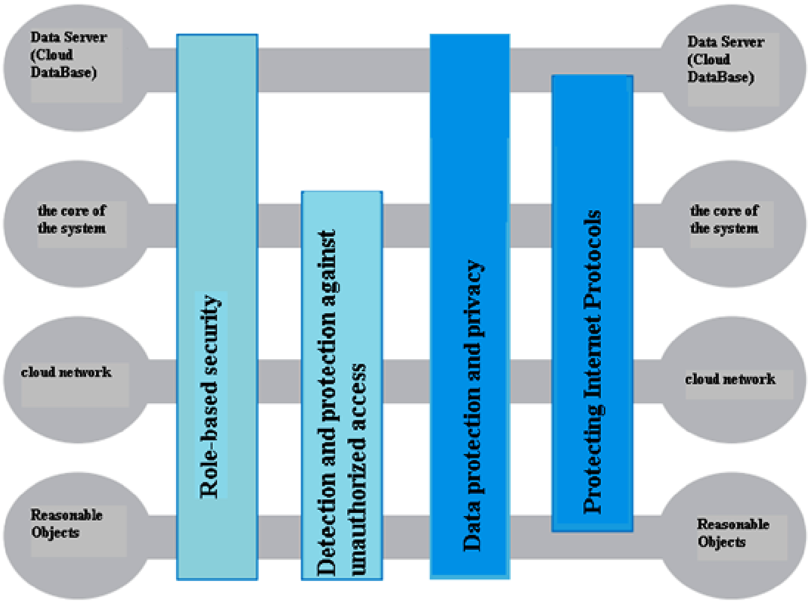

Data Server (Cloud DataBase)
the core of the system
cloud network
Reasonable Objects
Role-based security
Detection and protection against unauthorized access
Data protection and privacy
Protecting Internet Protocols
Data Server (Cloud DataBase)
the core of the system
cloud network
Reasonable Objects

Fig.2. Ways to transmit data through different types of networks and levels to ensure integrated system security

If the data is transmitted via the Internet Protocol IP continuously, there is the possibility of their so-called "tunneling" on the way from the device to the server. However, this is the only exception in this scheme, which roughly corresponds to the concept of integrated ultimate security.

An additional level of integrated security on the device-server route solves the following tasks: device authentication on the server; server authentication on the device; creating a session security key; data integrity; data confidentiality, if required.

Integrated Security Solutions in IoT Systems

More than 20 years have passed since Netscape introduced the first public version of SSL in 1995 [10].

The idea was simple: find a way to enable Internet users to safely, confidentially and continuously connect to remote servers to work with mail, Internet banking, e-commerce services regardless of who is the manufacturer of the hardware and operating system installed on software.

“Secure, confidential and uninterrupted” meant that the client has the ability to verify the authenticity of the server without disclosing passwords and confidential information to third parties, including Internet service providers and telecom operators. It also had to leave the fans of "eavesdrop" and hackers out of work. The simplest solution to this problem was to use the same unique security key on both sides of the communication channel.

However, a new problem arose: how to pass this unique security key without revealing it? A possible solution could be to use an additional channel. In the end, the banks send us the PIN codes of the cards in a separate letter, and some sites use our email to send us a temporary password during the registration process on the new service or to update the old password.

However, this was not a lightning process yet and, of course, it was impractical for updating session keys on an ongoing basis, a seamless and open to the user method.

This technology included the fundamental works of the founders of the asymmetric cryptography of Clifford Cocks, which they published more than 20 years before, in the interval between 1973 and 1977. They developed methods for calculating a unique security key, which can be shared through an open communication channel, without revealing any secret information, using two related objects (Fig. 3). So, if you see the abbreviation RSA or DH, remember these mathematicians. Since Cox worked for British intelligence, until recently his work and the very name of the scientist were classified, but, nevertheless, he also deserved our recognition [11].

Returning in 1995, we note that users still had the ability to securely verify the authenticity of the server and calculate the common key of the secure session used for data exchange.

As shown in the figure, servers do not send their public keys in their pure form, they send certificates that contain their public keys (Fig. 3).

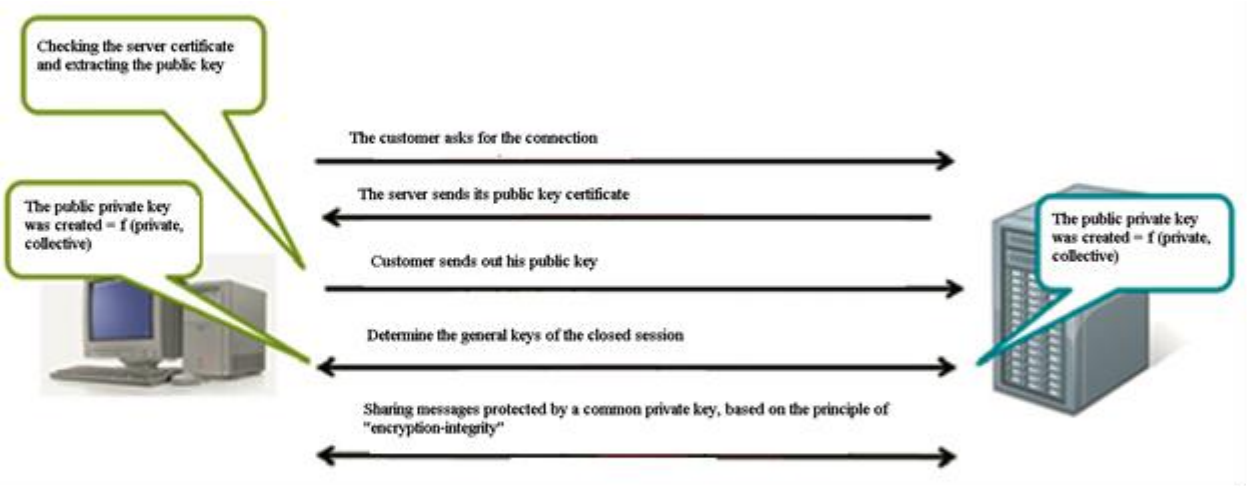

Checking the server certificate and extracting the public key
The public private key was created = f (private, collective)
The customer asks for the connection
The server sends its public key certificate
Customer sends out his public key
Determine the general keys of the closed session
Sharing messages protected by a common private key, based on the principle of "encryption-integrity"
The public private key was created = f (private, collective)

Fig.3. Servers send certificates that contain their public keys

Both sites have a public key, but the client needs to check and make sure which of these sites is genuine.

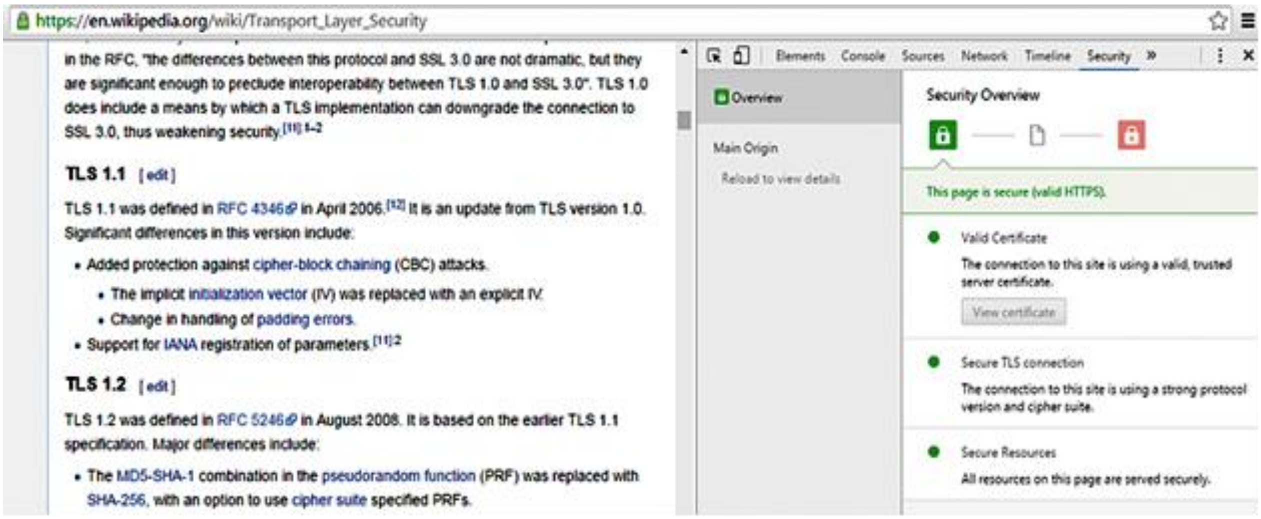
In order to carry out such checks, Certificate Authorities (CA) have been created. These are independent corporations that issue digital certificates that certify the ownership of the public key of the organization whose name is indicated in the certificate.

Let's assume that “www.mybank.com” wants to release the public key. At first, Mybank sends the key to the certification authority along with the accompanying documents and proof of their identity. The certificate authority will check whether “www.mybank.com” is the key owner and after this procedure will issue a digital certificate. It will contain, in addition to the public key “www.mybank.com”, the name of the company-owner, expiration dates and other related information, the private key of the certification authority itself. This certificate will then be sent back to “www.mybank.com”, and it will be sent to customers requesting connections. After receiving the client verifies the signature of the certificate using the public key of the certification authority, which, as a rule, is already installed in the browser. Thus, he will make sure that the public key contained in the certificate really belongs to the site “www.mybank.com”, to which it needs to be connected.

Despite the large number of proposals to improve the system, it is this architecture that currently allows you to ensure the security of Internet connections.

Below is a screen shot of a computer illustrating the request process (Figure 4).

Also, the RSA protocol is often replaced with the ECC protocol, since it creates keys of much shorter length and does not require complex calculations, while providing a higher level of security.



https://en.wikipedia.org/wiki/Transport_Layer_Security

in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". TLS 1.0 does include a means by which a TLS implementation can downgrade the connection to SSL 3.0, thus weakening security.[11] 1–2

TLS 1.1 [edit]

TLS 1.1 was defined in RFC 4346 in April 2006.[12] It is an update from TLS version 1.0. Significant differences in this version include:

- Added protection against cipher-block chaining (CBC) attacks.
  - The implicit initialization vector (IV) was replaced with an explicit IV.
  - Change in handling of padding errors.
- Support for IANA registration of parameters.[11]:2

TLS 1.2 [edit]

TLS 1.2 was defined in RFC 5246 in August 2008. It is based on the earlier TLS 1.1 specification. Major differences include:

- The MD5-SHA-1 combination in the pseudorandom function (PRF) was replaced with SHA-256, with an option to use cipher suite specified PRFs.

Security Overview

This page is secure (valid HTTPS).

● Valid Certificate

The connection to this site is using a valid, trusted server certificate.

● Secure TLS connection

The connection to this site is using a strong protocol version and cipher suite.

● Secure Resources

All resources on this page are served securely.

Fig.4. Servers send certificates that contain their public keys

Considering that the predicted number of devices that will be connected to the Internet is constantly growing, the size of the address space has already changed from 32 bits in IPv4 (4.3 billion unique addresses) to 128 bits in IPv6 (3.4 - 1038 unique addresses). And even so, the billions of sensors and devices already installed are still not IP compatible.

On the one hand, most of these devices can transmit data using wireless technologies and operate on batteries for 5–15 years, depending on the area of use. On the other hand, IP-compatible wireless technologies, such as 802.11 and 3G / 4G, which have been used for more than one year, greatly reduce the battery life of these devices.

At the same time, wireless technologies that rationally use batteries by reducing payloads, increasing the “hibernation” time, asynchronous mode and asymmetric connection, are often connected to gateways of LAN protocols such as Bluetooth, ZigBee, WmBUS, Z-Wave , Enocean, KNX, ioHomeControl, 802.15.4, and also without using gateways with LPWAN (Low Power Wide Area Network, energy-efficient long-range network) based on technologies such as Sigfox, LoRaWAN, NB-IoT and a few more.

Despite the recent implementation of the 6LoWPAN protocol in such standards as Thread and Bluetooth 4.2, it is expected that a huge number of sensors and devices that will be implemented under the slogan “Internet things "will not actually be IP compatible. Moreover, it will be at least until 2025, at least for reasons of backward compatibility with existing products. This means that all these billions of devices, from smart meters to industrial sensors, will not be able to use the IP standard to establish a TLS session with the server to which they connect.

Comprehensive Security and IoT Wireless Technologies

We are looking for a way to introduce an additional level of integrated security, shown in green in the figure, so that it is installed on top of the security systems of the rest of the connection (Fig. 5).

If we have at least one section where the IP standard is not supported, even if it is thin, with a low data transfer rate, then it will be an obstacle to transferring data all the way.

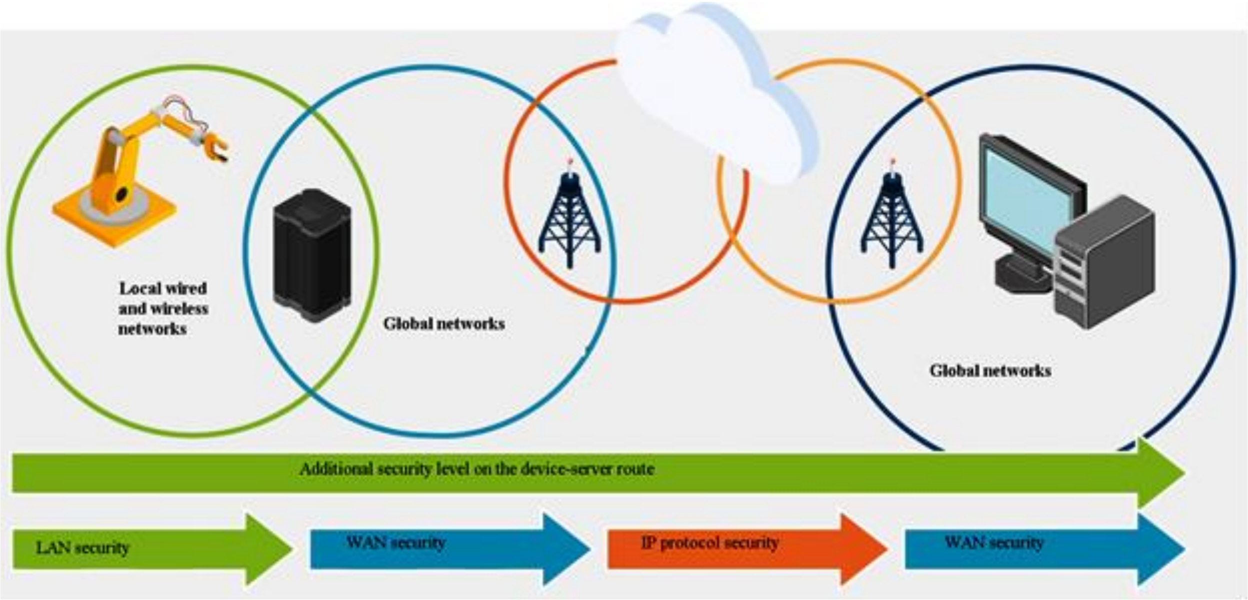


Fig.5. Additional level of integrated security

We offer a simple solution: if the existing IP TLS signal (Fig. 6) cannot overcome this obstacle due to the large amount of data, we create an adapted version of the TLS, which includes: using cryptographic algorithms with shorter keys (ECC), and no long key algorithms (RSA); smaller certificates; extended session key validity period; the ability of the sensor to check the server certificate offline, if required; a safe and easy way to personalize and store certificates along with session keys directly on the device or sensor; certification center services for the issuance and verification of ordered certificates.

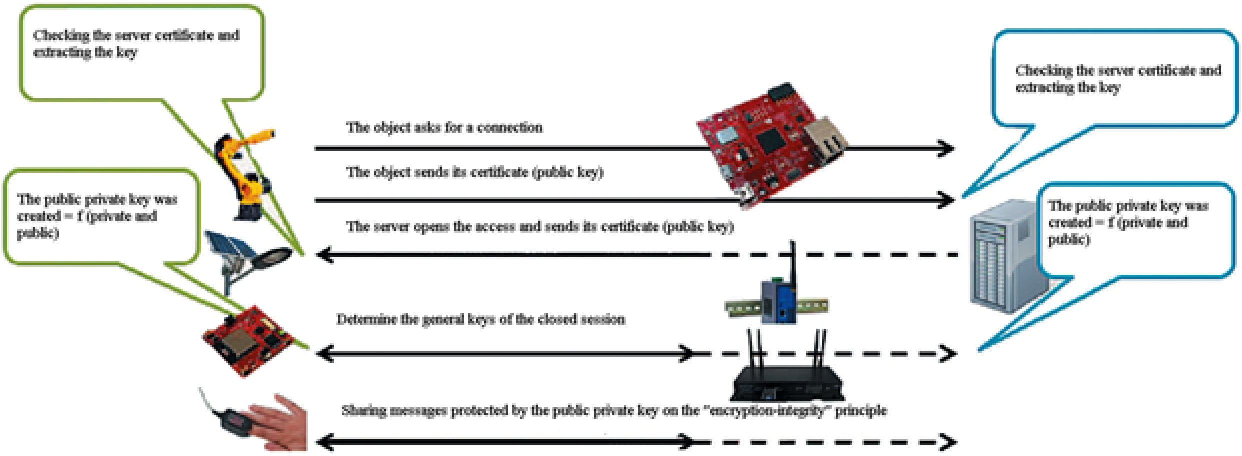

Checking the server certificate and extracting the key
The public private key was created = f (private and public)
The object asks for a connection
The object sends its certificate (public key)
The server opens the access and sends its certificate (public key)
Determine the general keys of the closed session
Sharing messages protected by the public private key on the "encryption-integrity" principle
Checking the server certificate and extracting the key
The public private key was created = f (private and public)

Fig.6. Adapted transport security

Such a TLS variant should perform the same functions as the original: mutual authentication; simple and automated allocation of resources to a sensor or device in a remote application; mechanisms for recalling a sensor or device from a remote application; ensuring the creation of an AES session key and secure exchange while respecting the integrity and encryption of the message.

Although many microprocessors can boast of energy efficient cryptographic stuffing, they do not solve real problems: someone has to personalize them at some point, and this creates certain inconveniences. They are not protected, and private keys can be read from their memory or calculated from dynamic changes in the supply current or even from electromagnetic radiation.

That is why Visa and SIM card chips do not use microcontrollers with a standard core like Cortex-M. And that is why such security elements are necessary.

These elements are miniature components that connect peripheral devices with receiving microcontrollers or microprocessors, and are responsible for personalized certificates; secure placement of private keys; management of cryptographic elements (Fig. 7).

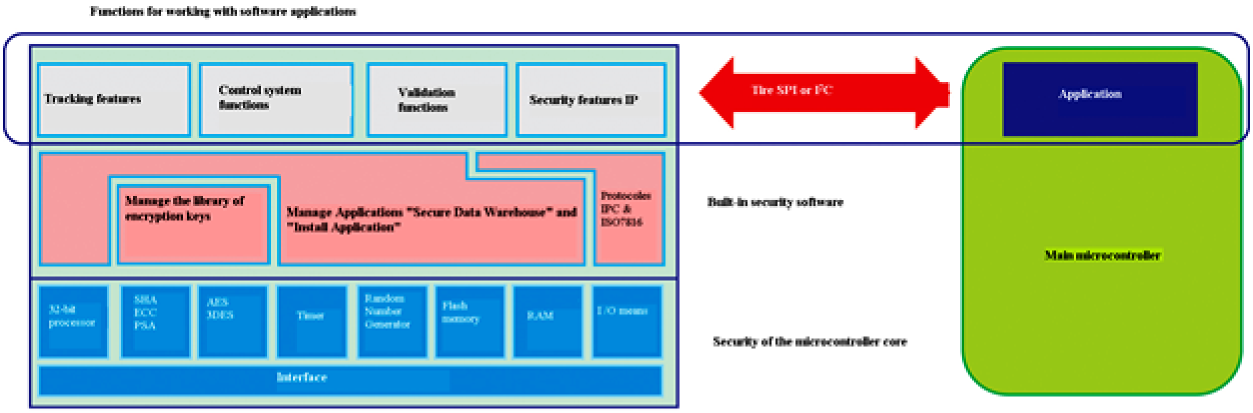


Fig.7. Integrated security system with unique identifiers and keys or certificates

All of this is part of the overall security solution. Our initial task was to reduce the cost and reduce the complexity of personalizing and resourcing devices, sensors, machines and mechanisms that are connected to local or remote servers. By changing the technologies mentioned above, we now have a complete set of solutions: TLS or similar stacks and APIs (Application Programming Interface), which carry out mutual authentication, distribution and update of session keys; security elements capable of accepting certificates and managing TLS source functions; ensuring security in the process of personalization - elements of protection before the production of the device, which eliminates the need to personalize the device itself; certificate authority services for the issuance and verification of certificates ordered during the entire 15-year service life of the connected device.

Typically, a gateway is a bridge connecting a local area network (LAN) and an application server via the Internet (IP network). Therefore, it is necessary to securely identify both the local server and the remote one.

Since the gateway and server are connected via IP, this can be done using TLS over any IP connection, be it Wi-Fi, Ethernet, or 3G / 4G cellular.

For such a case, we recommend using the security element personalized by Avnet Silica as an additional chip to the main processor, running under our UbiquiOS operating system and located in the gateway. It provides uninterrupted TLS connection to the server, which is managed by our API and performs the task of providing the gateway with resources via HTTPS or MQTTS.

As was shown above, the sensors often operate on batteries and must operate with small data on the volume. The 6LoWPAN protocol is an energy efficient version of the IPv6 protocol and is commonly used in the Thread network protocol. This allows you to directly connect the sensor and server using the TLS protocol.

For this option, we recommend using another security element, personalized by Avnet Silica, as an additional chip to the sensor microcontroller, also running under our UbiquiOS operating system. It manages the uninterrupted TLS connection provided by the gateway with a server that is controlled by our API and performs the task of securely providing the sensor with resources via HTTPS or MQTTS.

If the sensor does not support either the IP or the 6LoWPAN protocols, then you must install the TLS variant adapted for the local network technology directly between the sensor and the server.

In this case, we recommend using the same security element as an additional chip to the sensor microcontroller. The difference is that it manages our company's uninterrupted TLS connection option provided by the gateway with the server that is controlled by our API and performs the task of providing the sensor with resources with an optimal balance between security and power consumption, in accordance with the mechanisms used in the HTTPS or MQTTS protocols.

Conclusion

Already, IoT is changing the rules of the game in certain industries: it penetrates into inaccessible and previously impossible areas, improving the quality of life and increasing business efficiency. IoT technologies have found applications where they are profitable for business and convenient for people.

The advantages of LPWAN technology fit well into the needs of large-scale IoT implementation in industry, transport, security and dozens of other industries. Long range, high endpoint autonomy, easy deployment of an LPWA network and low infrastructure costs will give impetus to large-scale projects and the development of the Internet of Things.

By its very nature, the Internet is growing, developing and improving in such a way that its environment cannot be easy. This makes it harder to protect, but open standards and working code prove that security and privacy for everyone is achievable.

References

[1] Familiar, B. (2015). Microservices. [IoT and Azure], *Apress*, 69-93.

[2] Hu, F. (2016). Security and Privacy in Internet of Things (IoTs). [Models, Algorithms, and Implementations], *CRC Press*, 47-65.

[3] Rowland, C. (2015). Designing Connected Products. [UX for the Consumer Internet of Things]. *O'Reilly Media, Inc.*, 132-146.

[4] Perry, M. (2016). Evaluating and Choosing an IoT platform. *O'Reilly Media*, 152-163.

[5] Barlow, M. (2016). Are Your Networks Ready for the IoT. *O'Reilly Media*¸ 132-144.

[6] Zaeem, S. (2016). The Definitive Guide to the Internet of Things for Business. CTO, Aeris, 2nd Edition¸ 82-104.

[7] Gubbi, J. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, T. 29, № 7*, 1645-1660.

[8] Betts R. (2016). Architecting for the Internet of Things. *VoltDB Inc., O'Reilly Media Inc.*, 75- 83.

[9] Aggarwal N. (2016). Getting Analytics. *Tamr*, *O'Reilly Media Inc.*, 115- 143.

[10] Raso, O., P. Mlynek, R. Fujdiak, L. Pospichal, and P. Kubicek. (2015). "Implementation of Elliptic Curve Diffie Hellman in Ultra-Low Power Microcontroller". In 2015 38th International Conference on Telecommunications and Signal Processing (TSP), July 9th–11th, Prague, Czech Republic, 662–666.

[11] Phan, D., J. Yang, M. Clark, R. Grosu, J. Schierman, S. Smolka, and S. Stoller. (2017). "A Component-Based Simplex Architecture for High-Assurance Cyber-Physical Systems". In 17th International Conference on Application of Concurrency to System Design (ACSD), June 25th–30th, Zaragoza, Spain, 49–58.