Structure of information security subsystem in the systems of commercial energy resources accounting

D S Nikiforov*, A A Konev, M M Antonov and A A Shelupanov

Faculty of Security, Tomsk State University of Control Systems and Radioelectronics, 40 Lenin Ave., Tomsk 634050, Russian Federation

*E-mail: nds@csp.tusur.ru

Abstract. IoT (Internet of Things) systems are becoming popular and are widely used in various spheres of life today. However, sometimes the security of such systems leaves much to be desired. This article proposes an approach to the construction of IoT systems protection subsystem with an example of application of the proposed approach to the automated system of commercial energy accounting. A special feature of the approach is the method of choosing the means of protection based on the threat model for the system.

1. Introduction

Today, 2.9 billion people, or 40% of the world's population, are online. By 2020, at least 40 billion devices will be smarter with built-in processors. The impact of the Internet of Things (IoT) on our society will be unusual. IoT will affect most consumer and business sectors, education, health and other areas. However, this of course will also cause the problem from the point of view of information security. Not only the devices themselves will become more complex, but the interaction between devices and networks will also grow. Finally, with more data and assets at stake, the incentive for attackers will increase. Spending on cyberattacks in such conditions is estimated to reach about $ 2 trillion by 2020. Today IoT is just beginning to appear. Unfortunately, there is much room for improvement when considering security-related issues. Operational data published in a consistent manner clearly indicate that IoT security is a serious problem [1].

The emergence of smart environments, systems and services is driven by the development of the Internet of things. IoT devices produce large amounts of data, and this data is used to make critical decisions in many systems. The data obtained by these devices must meet various security requirements to be useful in practical scenarios. But safety and security risk awareness, which are not enough in the modern thinking of consumers and developers, is only a starting point. Once the security requirement is adopted, the economic question of who will pay for security and its maintenance will continue to be maintained. Without compliance with certain standards through third-party evaluation, the problem is expected to be difficult to monitor [2].

While it is recognized that security mechanisms and principles are needed across The IoT ecosystem, many of the internal features of IoT systems make them vulnerable to cyber security breaches. The purpose of this work is to increase the efficiency of the security subsystem in the IoT.
2. Existing solutions

Currently, the scientific community offers many different approaches to providing IoT devices authentication in the network. This is because most systems are used in areas related to accounting or control [3].

One of the requirements of IoT is the availability of data that allows the user to trust data about his origin and location. The low cost of many IoT devices and the fact that they can be deployed in unprotected locations require security protocols to be effective and safe from physical attacks.

Recently, several methods of data security using hardware security primitives have been proposed [4-6]. Other methods using the characteristics of the wireless channel have also been proposed. The authors [4] suggest using sensor PUF to determine the origin of the data in the IoT. However, if an attacker moves the PUF sensor from its original position, the circuit breaks down, meaning the data receiver will continue to take invalid sensor readings without knowing that the location of the data source has changed. Similarly, in [5] the authors suggest a scheme of data origin using wireless fingerprints. They use the received signal strength indicator (RSSI) values to create unique fingerprints. However, their scheme requires that touch devices store the private key locally. This requirement makes their Protocol vulnerable to physical attacks. Moreover, these methods use public key cryptography and have high energy and processing requirements.

It also offers design and implementation of the security scheme for the IoT based on the Protocol ECQV Implement Certificates and Datagram Transport Layer Security (DTLS). In this proposed security scheme, an elliptic curve-based ECQV cryptographic certificate plays a key role in enabling mutual authentication and key distribution between two resource-constrained IoT devices. And is, as IoT devices get ECQV implicit certificates and use them for the key exchange and authentication in DTLS.

There is information about comparing alternative options for secure communication of new IoT devices in existing networks that are based on asymmetric and symmetric cryptography. Although the security properties of both approaches are equivalent, an interesting trade-off arises between the Protocol properties and the properties of its implementation in current IoT devices. Indeed, while the asymmetric key approach takes on a lower overhead portion of the traffic (about 30%), we find that its implementation is significantly more energy-intensive and time-consuming due to the cost of cryptographic operations [7].

The disadvantages of the proposed solutions are their narrow focus [8]. The problem is not considered from the point of view of large distributed systems, but only as a set of low-power devices. The geographic scale of systems is usually limited to one building. But it is expected that IoT systems will be systems on a global scale, in the framework of the neighbourhood, city or even region. It is necessary to consider these aspects when building security subsystems of such systems [9].

3. Automated system of commercial energy accounting

3.1. System description

Examples of systems on a global scale on IoT can serve as an automated system of commercial energy accounting (ASCA). The class of these systems uses many metering devices, combined in the network, to collect data on resource consumption. The flow of this data is processed by the intermediate nodes and sent to the servers for analysis and storage.

Depending on the scope of use, the structure and scope of the ASCA may differ. ASCA of the enterprise, which uses large amounts of energy resources, often include separate subsystems of commercial and technical accounting. In a separate workshop of the enterprise it is possible to use only the system of technical accounting. In the public-sector institutions, or in the office there is no need for technical accounting, and on the scale of the housing and communal services of the city need commercial accounting. Accordingly, the ASCA uses primary measuring devices (AMR) of different accuracy classes and different devices of connection with objects and controllers.

A typical ASCA system consists of three levels:
• level of energy metering devices (AMR);
• the level of devices collecting and transmitting data (USPD);
• upper level system.
An example of the structure of a typical ASCA is shown in figure 1.

![Diagram of ASCA structure](image)

**Figure 1.** Typical scheme of ASCA.

This system is exposed to a range of different threats. Based on previous developments, models of threats to the confidentiality and integrity of information, as well as models of threats to the integrity of the system for ASCA were built. Based on these models were identified current threats.

The construction of the model of the information security subsystem is based on the classification of protection mechanisms depending on the elementary information flow and the type of threat.

To build a subsystem, you must:
• build a scheme of information flows in the system;
• for each information flow to determine the list of installed means of information protection (SCSI);
• list of information threats for each information flow.

To draw up a scheme of information flows, a model of the system, including a list of typical information flows, is needed. Thus, the scheme of information flows is a description of the real information flows in the system in the form of a structure consisting of typical elements (objects that store or transmit information, and subjects that process information) and typical communication channels between them.

3.2. Threats to the system
The threat model contains typical threats for typical information flows.

Threats of information at the hardware level (all devices of the system and protocols of the lower level belong to the hardware level of the system).
To address privacy threats, consider an example. As an example, a part of the scheme of information flows of ASCA (See figure 2), namely between:

- USPD;
- AMR;
- Engineer.

for which the types of threats to the confidentiality of information are defined.

![Diagram](image.png)

**Figure 2.** Information flows between the entities of ASCA.

Figure 2 shows two information flows:

1. between the service engineer and the USPD over the communication channel e1;
2. between the USPD and AMR of e2.

Violation of confidentiality of information for the first stream can occur in the following cases:

1. Sending USPD data to unauthorized engineer (substitution of subject "engineer");
2. Sending data to the unauthorized USPD by the engineer (substitution of the subject "USPD");
3. Data transmission via unauthorized communication channel (substitution/addition of communication channel);
4. Leakage data due to the properties of the communication channel (the affected channel).

For the second information flow the picture is similar:

1. Sending data to AMR unauthorized USPD (substitution of the subject "USPD");
2. Sending USPD data to unauthorized AMR (substitution of the subject "AMR");
3. Data transmission via unauthorized communication channel (substitution/addition of communication channel);
4. Leakage data due to the properties of the communication channel (the affected channel).

Similarly, for the threat of information integrity in the interaction of AMR and USPD are highlighted:

1. The threat of confidentiality of information due to the error of selecting the memory area for recording data received on USPD from AMR;
2. The threat of confidentiality of information due to the error of selecting the memory area for recording data received on the AMR from the USPD;
3. The threat of confidentiality of information due to high-frequency imposition of the communication channel between AMR and USPD;
4. The threat of confidentiality of information due to the presence of secondary electromagnetic communication channel between AMR and USPD;

The approach for determining threats to the system is based on another model described in [10].

Devices act as nodes of the graph, and communication channels act as edges. The attributes are the settings of all items. Accordingly, for each element of the system, the following threats are possible:

1. Delete items;
2. Add items;
3. Element attribute changes.

For example, we get 15 possible threats, among which are relevant:

1. The addition of a new engineer
2. Changing settings of a communication channel between the engineer and the DRC
3. Adding a new USPD
4. The removal of the USPD
5. To change the settings of the DRC
6. Adding a new AMR
7. Removal of AMR
8. Changing AMR settings
9. Adding a new communication channel between USPD and AMR
10. The removal of the communication channel between the USPD and AMR
11. Changing the settings of the communication channel between AMR

3.3. The subsystem of protection against selected threats
Let's move on to the subsystem of protection against selected threats

The subjects of access in this system are: customer application processes; Server application processes; users-customers of the energy company; system administrators; engineers. The objects of access in this system are: energy meters; data collection and transmission devices; servers. Client and Server application processes are assigned the appropriate roles that define the types of access: write – modify data; read. The approach to safety has been developed considering two widely used international standards IEC 62056 [11] and IEC 62541 [12]. The structure of the information security subsystem in the context of a typical energy accounting system is developed considering the considered standards.

The information security mechanisms to implement in the framework of the subsystem of protection: authorization of subjects of protection (1); authentication of subjects of protection (2); control of integrity of transmitted data (3); encryption of transmitted data (4); issuing and distribution of digital certificates (5); generation and distribution of keys (6); audit logging of events (7). The use of these mechanisms in the structure of the protection system is shown in figure 3. The numbers on the arrows and next to the objects indicate the appropriate mechanisms used by the objects of protection, including during the exchange of information [13].

![Figure 3. Security mechanisms in the security subsystem structure.](image-url)
The security subsystem architecture should be based on the following principles:

- The subsystem of protection is considered as a complex of means of protection aimed at ensuring the security of the information system and the information processed in it;
- each means of information protection is a set of protection mechanisms implemented in this tool;
- protection mechanisms should be present at each of the possible information flows of the “object-subject” and “subject-subject” types;
- each protection mechanism is designed to neutralize a specific threat existing on a given information flow.

When building a subsystem, information security specialists form a list of implemented security tools, based on their own experience. To date, there is no clear list of protection mechanisms implemented in a single means of protection, and their comparison with specific threats.

The classification of protection mechanisms depends directly on the threats. At the same time, each typical threat has its own protection mechanism.

Thus, the system is allocated 4 types of threats to the confidentiality of information. For each type of threat, a list of protection mechanisms must be defined. The following types of information security mechanisms in the system were identified:

- identification and authentication when accessing data
- data access control
- logging data access events
- to clear the memory after a data access
- data encryption during transmission

Similarly, the following types of security mechanisms for the system are distinguished:

- identification and authentication of subjects in the system
- event registration activity of entities in the system
- control of integrity of subjects of system

3.4. The proposed subsystem

The existing devices, which are part of the ASCA, do not have reliable protection mechanisms, as they are intended for use at industrial facilities and serve to control the use of resources, and not for their commercial accounting.

To ensure reliable authentication of devices in the ASCA proposed solution based on the recommendations of ITU-T G. 9903 02.2014. EAP-PSK Protocol is used as an authentication Protocol, which works on top of EAP Protocol, the capabilities of which have been expanded to work in networks with heterogeneous communication channels [14].

During the authentication process, devices receive encryption keys to communicate with the rest of the network (provided that the authentication is successful). The encryption algorithm is AES-CCM, which is a combination of two algorithms:

- AES-CTR is a stream cipher mode AES;
- AES-CBC-message authentication code counting algorithm.

This approach allows you to control the devices connected to the ASCA.

All devices connected to the system exchange information, the integrity and confidentiality of which is ensured by IPsec Protocol.

IPSec Protocol, ported to devices within the ASCA, provides mutual authentication of devices in the network using the IKEv2 Protocol. At the same time, there are options for working in which the network is configured using the EAP-PSK Protocol. During configuration, the device receives the network address and authentication keys, and then EAP-PSK crashes, and data transmission is performed by IPsec. The second option is the use of pre-installed certificates on the device. In this case, the initial setup is done manually, but the network does not need to use the EAP-PSK Protocol. Integrity control and data encryption during transmission is provided by the ESP Protocol, which is
used in IPsec at the transport layer. This Protocol provides protection not only for transmitted data, but also for network layer packet headers.

This approach allows to provide reliable authentication of devices in the AMR, to provide protection of transmitted data and provides many options for configuring the network mode but is not applicable for networks with heterogeneous communication channels. The EAP-PSK approach is not as flexible but is applicable to networks with heterogeneous communication channels.

3.5. **IPsec protocol**

Before the data transfer starts, a connection is established, which is called SA (Security Association). During connection establishment, the modes of operation and encryption algorithms are determined. SA is unidirectional, so two SAS are required for two-way communication [15].

The connection begins with mutual authentication of the parties, after which the channel settings (whether authentication, encryption, data integrity control) and the required Protocol (AH or ESP) are determined. After that, specific cryptographic algorithms are selected.

All SA are stored in the security Association Database (SAD) of the IPsec module. Each SA has a unique identifier consisting of three elements:

- The security parameters index SPI (Security Parameters Index);
- Destination IP address;
- The ID of the security Protocol.

Knowing these values, the IPsec module can be found in SAD

Security parameters database (SDP) which contains signatures of IP packets and performed on the packets with the specified signature, actions: drop the packet, send the packet over the IP Protocol, Apply IPsec Protocol.

SAD is a database in which is stored the active IPsec session. For each session its parameters are set:

- session direction (incoming or outgoing connection);
- cryptographic session key;
- cryptographic algorithms used;
- mode of operation of the connection (tunneling, transportation);
- the ARS status (enabled or disabled replay protection);
- number of the last sent package (Sq);
- working Protocol (AH/ESP).

The SPD is populated by the administrator and defines the Protocol policy. The SAD database is generated during the Protocol operation. The record is formed at the time of the session establishment before data transfer using the IKE-function of the ISAKMP Protocol. IPSec Protocol was implemented to test the operation of the proposed solution. To ensure the correct operation of our implementation, testing is necessary.

4. **Conclusion**

The presented model of the subsystem of information protection has a significant advantage in comparison with analogues. It consists in a detailed study of the specific elements of the model and the relationship between them, namely: this model considers all types of information threats to all kinds of information flows in virtual, electromagnetic, acoustic and species environments, a list of protection mechanisms that are aligned with the typical threats, neutralization of which they provide. This allows to improve the quality of the designed information security system and minimizes the impact of subjective aspects, such as the level of expertise of the expert. It is also worth noting that the proposed model can be used not only to build a system of protection of existing systems, but also to design new systems with the necessary protection mechanisms.

The construction of this model for AMR showed that one of the main protection mechanisms necessary to ensure the confidentiality and reliability of information is the mechanism of mutual authentication of devices used in the system.
The existing devices, which are part of the AMR, do not have reliable protection mechanisms, as they are intended for use at industrial facilities and serve to control the use of resources, and not for their commercial accounting.

IPsec allows you to flexibly configure security policy at the expense of your SDP database. We can say that IPsec allows us to implement the approach proposed in the DLMS standard. The SDP database is filled with signatures that allow you to determine where (from the server, client or other device) the request comes from, and set the level of connection security. The determination is based on the addresses from which the request is made, and the ports to which they are received. Accordingly, when requesting accounting data via the web-interface, the authentication module does not use IPsec protection mechanisms, the connection is made over the IP Protocol (the analogue of the no security level offered by DLMS).

If the controller sends data to a server, the controller confirms its authenticity by means of IPsec authentication. In this case, the IKEv2 Protocol for authentication is working. And a connection is established, which guarantees the integrity of the transmitted information using the ESP Protocol in transport mode (analog of the LLS level).

If the Server sends any control commands or settings, a secure connection is established with the mutual authentication of the parties (IKEv2) and the subsequent installation of an encrypted communication channel over the ESP Protocol in combined mode: transport mode for integrity control inside the tunnel, which provides encryption (HLS analog).

This approach allowed to implement protection mechanisms that provide the proper level of protection, while reducing the load on the device by selective use of various protocols in the exchange of information.

Acknowledgments
This work was partially supported by the Ministry of Education and Science of Russia, Government Order no. 2.8172.2017/8.9 (TUSUR).

References

[1] Medwed M 2016 IoT Security Challenges and Ways Forward 16 Proceedings of the 6th International Workshop on Trustworthy Embedded Devices 55
[2] Minoli D, Sohraby K and Occhiogrosso B 2017 IoT security (IoTsec) mechanisms for e-health and ambient assisted living applications. Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies 13
[3] Muhammad N Aman, Kee Chaing Chua and Biplab Sikdar 2017 Secure Data Provenance for the Internet of Things. Proceedings of the 3rd ACM International Workshop 11
[4] Kanuparthi A 2013 Hardware and Embedded Security in the Context of Internet of Things Proc. ACM CyCAR
[5] Ali S T 2013 Securing Data Provenance in Body Area Networks using Lightweight Wireless Link Fingerprints Proc. Trusted
[6] Cheng D 2015 Wireless Device Authentication Using Acoustic Hardware Fingerprints Proc. Int. Conf. on Big Data Computing and Communications
[7] Duy An Ha, Kha Tho Nguyen and John K Zao 2016 Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol. SoICT '16 Proceedings of the Seventh Symposium on Information and Communication Technology 173
[8] Internet of Things Architecture (IOT-A) Project Deliverable D Initial Architectural Reference Model for IoT
[9] Minoli D, Enterprise Architecture A thru Z: Frameworks Business Process Modeling, SOA, and Infrastructure Technology Auerbach
[10] Novokhrestov A, Konev A 2016 Mathematical model of threats to information systems AIP conference proceedings 1772 060015

[11] Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer International Electrotechnical Commission – 03.2016 – 420 c.

[12] OPC Unified ArchitectureSpecification Part 2: Security Model OPC Foundation – 25.11.2015 – 39

[13] Novohrestov A K and Konev A A 2014 Quality assessment of computer network security Dynamic of systems, mechanisms and machines 85-87

[14] Antonov M M, Konev A A, Nikiforov D S and Cherepanov S A 2016 Organization of the protected heterogeneous network in the automated systems of commercial accounting of energy resources Reports of TUSUR [in Russian – Dokladi TUSURa] 19(3) 107-110

[15] RFC 4301 Security Architecture for the Internet Protocol