Smart home security management

T. Tatarnikova, B. Sovetov

1 Department of information technologies and security systems, Russian state hydrometeorological University, 79 Voronezhskaya ulitsa, Saint-Petersburg, 195027, Russian Federation
2 Department of information systems, Saint Petersburg Electrotechnical University "LETI", 5 ulitsa Professora Popova, 197376, Saint-Petersburg, Russian Federation

tm-tatarn@yandex.ru, bysovetov@mail.ru

Abstract. The problem of ensuring the information security of the smart home is discussed, the main vulnerabilities and the consequences they can cause are listed. Mechanisms for protecting information in the smart home system based on the characteristics of consumed resources: energy, time, computing power, are proposed. A description of the smart home system assembled model is presented, and consumed resources characteristics allowing reasonable choice of the method for protecting information transmitted by devices over open channels are measured by using this model.

1. Introduction
Connecting smart devices to the World Wide Web requires ensuring the security of data transmitted through the "device-device", "device-server", "device-user" channels. Attackers can not only steal confidential information, but also take control over the device.

The main security vulnerabilities of the smart home system are [1]:
- Use of own software by manufacturers of smart home systems, which complicates the interaction between devices from different manufacturers. In addition, software is often closed source, which in turn complicates the finding of vulnerabilities.
- Insecurity of traffic, which allows attackers to receive data transmitted by devices.
- Lack of an authentication mechanism, which allows attackers to take control over the device.
- The listed vulnerabilities can lead to the following consequences:
  - Malfunction of the device.
  - Violation of confidentiality, integrity and availability of information.
  - Interception of control over the device by an attacker.

Most of these consequences are explained by the low performance of the devices, which does not allow fully implementing information protection [2,3].

There are several approaches to securing smart home devices. All of them differ in algorithms, threat models, but what is more significant for systems of this kind, they differ in the values of the consumed resources: energy, time, computing power.

This paper proposes methods for protecting information transmitted by devices through open channels in a smart home system, and the choice of these methods is justified experimentally. Firstly, a mock-up of a smart home system is assembled, and secondly, the consumed resources are measured.
The present report is devoted to the features of the model implementation and conduction of experiments on it to substantiate information protection methods.

2. Features of the smart home system model implementation.
As a part of the smart home system model, the following software and hardware modules are implemented (Fig. 1) [4]:

- The controller with temperature and pressure sensors connected to it.
- Server.
- Database.
- User interface.

Arduino Uno is used as a controller allowing interacting with sensors. The controller work is organized in an endless loop, i.e. sensors are constantly polled and user connections are checked. A relay is used to control the external devices opening/closing.

The server is implemented in php using the MVC pattern model-view-controller allowing to logically separate the database interaction, user interface and application logic [5].

![Figure 1. The modules interaction scheme in the smart home system model](image)

The database is used to solve the problem of data storage and access control. The database includes the following tables: user data, access levels, application supported actions, readings and the history of their changes.

The user interface is a web application that contains the registration, authorization and main pages where data from the controller is displayed. The application greets users with an authorization window where users can enter their login information or register to get started. After logging in, the user accesses the application main page. Here user has an access to data from sensors, which are updated every few seconds. Data refresh requests are made using server requests. Also on this page it is possible to set the temperature that is to be maintained by turning on the device through the relay on the controller. Another available possibility is to view the history of temperature and humidity readings changes.

3. Recommended protection mechanisms of the smart home system.
Since the controller is a low-power device, it is not able to support the https connection. Therefore, to transmit data from the server to the controller, we use the http protocol with an additional solution of encryption problems and integrity checking of data transmitted over the Internet. Symmetric algorithms are recommended for encryption. To ensure the transmitted data integrity, the imitation insert is done, which in comparison with an electronic digital signature requires less computing power and less memory.

User authentication (access to the smart home system) is implemented on the server using the https protocol, which protects user data when transmitting them over open channels. Also, the server
requests data from the controller and transfer it to the user, which allows partially removing load from the controller. This approach is widely used when using low-power devices.

Each action, such as home page opening or requesting the data update from sensors, has its own access level to share the access. So, all actions above level 1 can only be performed by registered users. If an unregistered user, for example, requests data from sensors, he is redirected to the access error page.

Thus, ensuring information security of a smart home system includes the following mechanisms:

- Interaction between the client and the server is carried out through the HTTPS protocol, which using the SSL/TLS cryptographic protocols provides 3 levels of protection:
  1. Data encryption, which allows avoiding data interception;
  2. Fixation of any data changes, which ensures their integrity and preservation;
  3. Authentication, which protects against user redirection.
- The interaction between the controller and the server is carried out via the HTTP protocol, but the data is encrypted and protected from being changed by an authenticated encryption.
- Encryption/decryption of data transmitted between the controller and the server is implemented by a symmetric cryptographic scheme.

It is important to use the strongest ciphers and their protection for control packages. Security requirements for information packages are lower, but the processing speed and size requirements are higher.

4. Description of the experiment for measuring the consumed resources using the smart home model. Analysis of results

The resources consumed by the system are estimated by using the following characteristics:

1. System response time $t$, in ms, which shows the expected response time from the system to the user request.
2. Single request energy consumption $E$, in W, which shows the value of the power spent by the system to process one request.
3. System load $P$, in bytes, which shows how much data is transmitted over the network with a single request.

The system response is evaluated by measuring the time from the moment of sending a user request to receiving a response in the client computer browser. For this, the standard developer panel is used allowing viewing the request time.

To estimate the power consumption, a multimeter is used allowing measuring the current consumed by the Arduino during the request execution and calculating the power consumption.

The network load is estimated through the packages size sent from the server to the controller and vice versa. This characteristic strictly depends on the selected encryption algorithms and imitation insert.

Before the encryption, the data is 4 bytes long and contains information about the temperature maintained in the room. The size of the imitation insert does not depend on the encryption algorithm and is equal to 20 bytes.

Data is transmitted from the controller to the server in the same format, but the data size before the encryption is 14 bytes.

The measured characteristics of the smart home system without the implementation of transmitted data protection mechanisms are as follows: $t$ equals 60 ms, where 5 ms is spent on controller processing; $E$ equals $5.75 \times 10^{-3}$ W/request, calculated by the equation $E = UIt$, where $U$ is the voltage [V], $I$ is the current, [A], $t$ is the single request time; and 32 data bits are transmitted with a single request.

Measurements show that while waiting, the system consumption is 0.19 A, and when the request is being processed, the consumption rises up to 0.23 A, which allows us to conclude that the power consumption depends on the request processing time.
The SHA library is used for the protection implementation. The library contains the SHA-1, SHA-256 and SHA-512 algorithms. The hmac versions of the algorithms are also supported. Encryption takes place using the AESLib, ArduinoDES and XTEA libraries. These libraries contain symmetric encryption algorithms: AES 128, AES 192, AES 256, DES, TDES, XTEA. Table 1 shows the sizes of packages sent from server to controller and from controller to server.

| Encryption algorithm | Server-Controller | Controller-Server |
|----------------------|-------------------|-------------------|
| AES 128              | 36                | 36                |
| AES 192              | 44                | 44                |
| AES 256              | 52                | 52                |
| DES                  | 28                | 36                |
| TDES                 | 28                | 36                |
| XTEA                 | 28                | 36                |

The time from the moment of sending a user request to receiving a response in the client computer browser is measured to estimate $t$. Also, for the sake of completeness, the request execution time on the controller from the moment of receiving a user’s request to sending data to the server is measured. The $t$ estimate is an averaged value of 10 queries. Fig. 2 shows the results of $t$ measurements for packages.

The energy consumption is measured using a multimeter in such a way that the current consumed by the controller is measured during the request execution time, and then the calculation of the power consumption is made. Fig. 3 shows the results of $E$ measurements for information and control packages.
Figure 4 shows the results of $P$ measurements for information and control packages.

![Figure 4. Results of $P$ measurements](image)

The results of experiments carried out on a mock-up of a smart home system show that XTEA is the most suitable algorithm for low-power devices. It provides the fastest encryption with the lowest power consumption. However, XTEA does not have the highest cryptographic strength, which limits its use for important data. The use of AES family of algorithms is also justified, since the results are not particularly inferior to XTEA, and moreover AES is characterized by the high cryptographic strength and can be recommended for critical data transmission.

5. Conclusion

The mechanisms proposed in the work allow ensuring information security of a smart home and take into account the resources consumed by the system, such as the response time, energy consumption and system load. Thus, the choice of protection mechanisms is substantiated by the results of experiments carried out on a smart home system model.

Imitation insert obviously increases all values of the consumed resources, since the control package size increases from 1.6 to 6 times. The decision on the imitation insert usage at the "device-device" and "device-server" sections is made depending on the object of smart home system implementation.

References

[1]. Tatarnikova T.M., Dziubenko I.N. 2018 IoT system for detecting dangerous substances by smell. Information and Control Systems. 2018. [Informatsionno-upravliaiushchie sistemy – in Russian] 284. doi: 10.15217/issn1684-8853.2018.2.84

[2]. Sovetov B., Tatarnikova T. 2020 Metric properties of building a list of trusted nodes during selection of data transfer routes in wireless sensor networks. MICSECS 2019 - Proceedings of the 11th Majorov International Conference on Software Engineering and Computer Systems.

[3]. Tatarnikova T. M. 2019 Limitations of information leakage through the non-obvious features of the Android 5 smartphone. Information and Control Systems. [Informatsionno-upravliaiushchie sistemy – in Russian] 24. doi:10.31799/16848853-2019-5-24-29.

[4]. Hersent O., Boswarthick D., Elloumi O. The Internet of Things: Key Applications and Protocols. Willey Publ., 2012.

[5]. Bogatyrev V. A., Vinokurova M. S. 2017 Control and Safety of Operation of Duplicated Computer Systems. Communications in Computer and Information Science, IET – 2017 (vol. 700), pp. 331-342.