UDC 629.735.018.7.015.3.025.1

V.M. Korchan, PhD, I.V. Morozova
(National Aviation University, Ukraine)

Method for modifying the architecture of digital objects to improve network security

This article describes a method for modifying the architecture of digital objects in order to increase trust and security in the exchange of data between elements of the digital object architecture and IoT devices. The purpose of the proposed method and the corresponding mathematical model is to protect the privacy of the Internet of Things in the application domain.

Security enhancement scheme for resolution system

Proposed security enhancement scheme for the resolution system. LHR and GHR servers have their own predefined keys ΨLHR, GHR used in messaging and processes authentication. Each server (LHR and GHR) generates a random number with a predefined frequency of RLHR and RGHR respectively. The generated numbers are used for encryption and decryption.

$$L_{GHR} = \text{Rand}\,(R_{GHR}), \qquad (1)$$

$$L_{LHR} = \text{Rand}\,(R_{LHR}). \qquad (2)$$

The LHR server performs a sequence of actions that combines the identification number of the LHR server with a randomly generated number at a predetermined frequency and a given request number.

$$M_1^{?_1} \{ID_{LHR}, L_{LHR}, Q_n\}. \qquad (3)$$

The message M1 is encrypted using the public key γ1. The LHR server then determines the required set of message data to be exchanged with the centralized GHR registry:

$$R \rightarrow R : < ?_1^{\gamma 1}, ?_2^{\gamma 1}, ?_3^{\gamma 1}, \ldots., ?_n^{\gamma 1} >. \quad (4)$$

The GHR receives the data set and decrypts the M1 message using the pre-shared key. The decrypted message looks like this:

$$\left[M_1^{?_1}\right] ?^1 ?\; ID_{LHR}, L_{LHR}, Q_n\,. \qquad (5)$$

The GHR server then retrieves the LHR ID to check server access permissions:

$$\mathrm{ID}_{\mathrm{host,app-serv}} \,?\, \mathrm{ID}_{\mathrm{host}} \,?\, \mathrm{L}_{\mathrm{GHR}},$$
$$\mathrm{ID}_{\mathrm{IP,\ app-serv}} \,?\, \mathrm{Q_n} \,||\, (\mathrm{ID}_{\mathrm{host,app-serv}} \,?\, \mathrm{L}_{\mathrm{LHR}}). \qquad (6)$$

Next, the GHR server calculates the hash sum and the digital signature. The hash sum, which is calculated using the hash function, is a numeric representation of the content of the message. Its length is predetermined:

$$\text{[illegible]}_{\mathrm{GHR}} \text{[illegible]} \text{[illegible]} \mathrm{Mess} \text{[illegible]} \mathrm{Size}[\mathrm{ID}_{\mathrm{IP,\ app-serv}}] \text{[illegible]}^{\text{[illegible]}}{}_{\mathrm{GHR}} \text{[illegible]}^{\text{[illegible]}} \text{[illegible]}^{\text{[illegible]}1},$$

$$\mathrm{Mess} \text{[illegible]} \mathrm{Size}[\mathrm{ID}_{\mathrm{IP,\ app-serv}}] \text{[illegible]} \text{[illegible]}_{\mathrm{GHR}}. \qquad (7)$$

The GHR server returns PGHR and IDIP, app-serv to the LHR server, which is a confirmation of the signatures.

$$\mathrm{ID}_{\mathrm{IP,\ act}} \text{[illegible]} Q_n \,||\, [\mathrm{ID}_{\mathrm{host,\ app\text{-}serv}} \text{[illegible]} L_{\mathrm{LHR}} \text{[illegible]} L_{\mathrm{LHR}}] \text{[illegible]} Q_n \,||\, \mathrm{ID}_{\mathrm{host,\ app\text{-}serv}}. \qquad (8)$$

To solve security issues in the area between the LHR and GHR servers, the presented Handle system defines two types of messages involved in the exchange. The first type of message is sent by the LHR server to the GHR server and encrypted with a predefined key. The second type of message is transmitted from the GHR server to the LHR server and contains digital signatures.

The presented security model in the proposed Handle system uses a minimum number of messages to ensure the authentication process. This scheme is effective for use in IoT devices, because it allows you to reduce the total amount of data transferred and at the same time reduce network delays in the security process.

The Digital Object Architecture Identification Service can be used to determine what information can be shared, with whom the information can be shared, and how the information will be transferred. Compatible applications can be developed by interacting with each individual application, providing an integrated interoperability service based on real-time data from each individual application.

Conclusion

The article presents a description of the structure of a typical IoT device and the resolution process based on the architecture of digital objects. Typical examples of the implementation of the described methods and the interaction of the Internet device are considered things with digital object architecture components. A model of a resolution system for digital object identifiers is proposed as a queuing system, on the basis of which an optimization experiment is performed and a configuration of the resolution system is obtained, which makes it possible to reduce the time for resolution of a device identifier.

References

1. Jena, A.K. A. Modeling and Evaluation of Network Applications and Services / A.K. Jena, P. Pruthi, A. Popescu // Proceedings of the RVK 99 Conference. – Ronneby, Sweden. – June 1999
2. Kirichek, R. False clouds for Internet of Things and methods of protection / R. Kirichek, V. Kulik, A. Koucheryavy // 18th International Conference on Advanced Communication Technology (ICACT). – 2016. – P. 201–205.
3. Kirichek, R. Model networks for Internet of Things and SDN / R. Kirichek, A. Vladyko, M. Zakharov, A. Koucheryavy // 18th International Conference on Advanced Communication Technology (ICACT), 2016. – IEEE, 2016. – P. 76–79.
4. Koo, J. Interoperability of device identification in heterogeneous IoT platforms / J. Koo, Y.G. Kim // 2017 13th International Computer Engineering Conference (ICENCO). – IEEE, 2017. – P. 26-29.
5. Wang, Ya. A privacy enhanced DNS scheme for the Internet of Things / Ya. Wang, Q. Wen // International Conference on Communication Technology and Application (ICCTA 2011). – 2011. – P. 699-702.