SECURE AUTHENTICATION IN IOT

Radchenko V.O., Afanasieva A.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Authentication also prevents hackers from attempting to appropriate the identity of IoT devices to gain access to data or the broader corporate network [1, 2].

The purpose of the report is to analyze how to protect data sent from and to the internet of things by securing authentication.

Recently, the number of smart things, such as cameras, various sensors, smart light bulbs, switches, and more, has been growing steadily [3]. These things have constant access to the Internet and actively share data for analytics with apps. In fact, there is more strategically important data, such as sensor readings about patient health. There are three types of authorization, the first one is authentication by username and password. The point is that when a device connects to the link broker (devices never connect directly), it sends a username and password to the link broker using the connect command. The password is sent in plain text if it is not encrypted.

The second one is authentication by access token: this option also uses the connect command. When this mechanism is enabled, the device sends an OTP request to the IoT application, via a broker. The application generates a one-time password and sends it to the owner's trusted device, and the application also sends a notification to the device we want to authorize. And the third one is authentication based on a one-time password. When this mechanism is enabled, the device sends an OTP request to the IoT application, via the broker. The application generates a one-time password and sends it to the owner's trusted device, and the application sends a notification to the device that we want to authenticate. IT admins who decide which IoT authentication method to use must consider the IoT device type, the data it transmits over the network and the device's location.

References

1. Tkachov V. Principles of Constructing an Overlay Network Based on Cellular Communication Systems for Secure Control of Intelligent Mobile Objects / Vitalii Tkachov, Andriy Kovalenko, Mykhailo Hunko and Kateryna Hvozdetska // Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2020. – К.: ООО "Инжиниринг", 2020. – С. 51-55.

2. Tkachov V. Method to Determine Fault-Tolerant Performance Probability of High-Survivability Computer Network based on Mobile Platform / Vitalii Tkachov, Mykhailo Hunko, Olga Morozova, Artem Tetskyi, Andrii Nicheporuk // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 05-07 oct. 2021, Kharkiv.

3. Tkachov V. Interval Evaluation of the Survival Rate of the Computer Network On the Basis of Highly Mobile Units With Normal Distribution of Work / V. Tkachov, O. Yeroshenko, L. Bukharova // Trends in science and practice of today. Abstracts of V International Scientific and Practical Conference. Ankara, Turkey. 2021. Pp. 409.