Contribution ID: **339**   Type: **not specified**

Continuous Authentication in Internet of Things Systems

Thursday, 6 July 2023 17:45 (15 minutes)

An essential part of any system's security architecture is an authentication mechanism –some algorithm or combination of algorithms making sure that only legitimate users can gain access to the system. Continuous authentication (CA) is a new approach to user authentication in distributed systems. Its main principle is that unlike a "traditional" approach, where a user is only authenticated once at the beginning of a session, in CA the user's identity is re-verified throughout the entire session. This means that even if a user's device becomes compromised after a successful log-in, unauthorized access to the system can still be prevented. CA is a part of a larger cybersecurity doctrine known as zero-trust architecture, or ZTA.

Internet of Things (IoT) systems are growing more common and more sophisticated by the day; consequently, the need to provide security for them, including reliable authentication systems, is also becoming more urgent. On the other hand, IoT devices also present unique challenges in regard to implementation of authentication mechanisms; in particular, they might lack computing power necessary for more complex algorithms, as well as conventional user interfaces such as keyboards or touchscreens.

In this paper, distributed system continuous authentication algorithms that can be used with IoT systems are investigated. They include methods using such technologies as blockchain, machine learning, and biometrics. Based on the results of the analysis, new approaches to the task of implementing CA in an IoT context are suggested.

Summary

Primary authors: MATIUSHIN, Iurii (Saint Petersburg State University); KORKHOV, Vladimir (St. Petersburg State University)

Presenter: MATIUSHIN, Iurii (Saint Petersburg State University)

Session Classification: Student section