SECURING MODERN IOT SYSTEMS USING LIGHTWEIGHT AUTHENTICATION SCHEMES

Ahmed Yaser Fahad Alsahlani , Alexandru Popa
Department of computer science, Faculty of mathematics and computer science,
University of Bucharest, Bucharest, Romania
Email: a.myphd@yahoo.com

Abstract

Communicating smart devices in the Internet of Things (IoT) environment using cloud technology brings numerous benefits in various fields and making human daily life more convenient. Since the occurrence of the novel COVID-19, the demand for remotely managed systems will significantly increase. The aim is to reduce the harmful consequences of physical distancing and to increase the systems' efficiency as well. In such systems, sharing information among registered entities over public channel brings numerous security risks e.g., reply, impersonation, DOS, man-in-the-middle, and lost/stolen smart card attacks. To accord with these attacks, authentication is one of most important security services that can protect the systems against these potential attacks. It is worth mentioning that the perfect authentication scheme should be secure against potential attacks and lightweight as well. In other words, it is meaningless to design a secure and robust scheme where no IoT-sensor can perform required computations. Hence, it is utmost important to design a secure as well as lightweight authentication scheme for the resources-constrained IoT-sensors which is challenging objective to be achieved. However, most of the existing authentication schemes suffer from several weaknesses and are still incomplete.

Keywords: Security analysis; Security; Lightweight; Internet of Things (IoT); Real-time data access
Domain: computer science.
Section: New (2020) thesis proposals

Introduction

The Internet of Things (IoT) based systems provide promising solution in various fields such as military, smart city, healthcare, traffic monitoring, smart grid, etc. [1, 2, 3, 4, 5, 6, 7]. How-ever, securing such systems is a crucial objective to be accomplished. Authentication is one of the most important security services that can secure the system resources and prevent unauthorized access. In this context, various authentication schemes were proposed by researchers, each having its pros and cons. Some of the proposed schemes are using public key infrastructure (PKI) and some other using symmetric key infrastructure (SKI). Further, the scheme designer uses various security factors i.e., something you know, e.g., password; something you have, e.g., smart-card; and something you are, e.g., biometric information. Accordingly, the scheme will be single, two-factor, or multi-factor based on the number of adopted security factors. Furthermore, the authentication schemes are compared to each other based on the security features that each scheme achieved including the attacks they resist, mutual authentication among system entities and session key agreement, etc.

Motivation

The COVID-19 pandemic [8, 9] has forced many changes onto the way we live and work. Physical distancing, travel restrictions and other health measures have bad consequences on the productivity of many organizations. Whenever it possible, many organizations are changed to manage their activities via online communications. However, this huge shift toward remote work expands the need for security solutions to withstand potential risks. Unfortunately, most of the existing authentication schemes are suffering from several weaknesses that need to be addressed.

Methodology of Research

At the first stage of our PhD, we intend to study the most recent authentication schemes that designed for IoT systems and pointed out their associated weaknesses. Then, we aim to address these weaknesses and propose a new authentication schemes which can efficiently respond to the market needs.

References

[1] M. Winkler, K.-D. Tuchs, K. Hughes, G. Barclay, Theoretical and practical aspects of military wireless sensor networks, Journal of Telecommunications and Information Technology (2008) 37–45.
[2] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya, M. Conti, Iot-enabled smart lighting systems for smart cities, in: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2018, pp. 639–645.
[3] M. M. Rathore, A. Ahmad, A. Paul, S. Rho, Urban planning and building smart cities based on the internet of things using big data analytics, Computer Networks 101 (2016) 63–80.
[4] Y. Yuehong, Y. Zeng, X. Chen, Y. Fan, The internet of things in healthcare: An overview, Journal of Industrial Information Integration 1 (2016) 3–13.
[5] M. Bottero, B. Dalla Chiara, F. P. Deflorio, Wireless sensor networks for traffic monitoring in a logistic centre, Transportation Research Part C: Emerging Technologies 26 (2013) 99–124.
[6] S. S. Reka, T. Dragicevic, Future effectual role of energy delivery: A comprehensive review of internet of things and smart grid, Renewable and Sustainable Energy Reviews 91 (2018) 90–108.
[7] D. Kolokotsa, The role of smart grids in the building sector, Energy and Buildings 116 (2016) 703–708.
[8] C.-C. Lai, T.-P. Shih, W.-C. Ko, H.-J. Tang, P.-R. Hsueh, Severe acute respiratory syndrome coronavirus 2 (sars-cov-2) and corona virus disease-2019 (covid-19): the epidemic and the challenges, International journal of antimicrobial agents (2020) 105924.
[9] WHO, novel-coronavirus, 2020. URL:https://www.who.int/emergencies/diseases/novel-coronavirus-2019.