عنوان مقاله:

On the Security of Permutation Based Authentication Protocols for Internet of Things Applications: The Case of Huang et al.'s Protocol

محل انتشار:

مجله محاسبات و امنیت, دوره 3, شماره 4 (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:

Samad Rostampour - *Department of Computer Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran*

Nasour Bagheri - *Department of Electrical Engineering, Shahid Rajaee Teachers Training University, Tehran, Iran*

Mehdi Hosseinzadeh - *Department of Electrical Engineering, Shahid Rajaee Teachers Training University, Tehran, Iran*

Ahmad Khademzadeh - *Iran Telecommunication Research Center, Tehran, Iran*

خلاصه مقاله:

The Internet of Things (IoT) is a new technology, which enables objects to exchange data via the Internet. Authentication process is a method to prevent an unauthorized access to the IoT systems. The using of bit-wise functions such as XOR, Shift and Rotation could decrease the cost of authentication protocols. On the other hand, the simple operations usually could not provide an acceptable security level. Therefore, the researchers try to improve the security level by creating new permutation functions. In this paper, we evaluate some permutation functions and analyze a protocol which recently has been proposed by Huang et al. We prove that their protocol is vulnerable to the disclosure and the impersonation attacks and an adversary can clone a valid tag easily. The complexity of the .proposed attack is low and attack method works efficiently for the secret keys and ID numbers with variable length

کلمات کلیدی:

Internet of Things, RFID, Security, Authenti cation

لینک ثابت مقاله در پایگاه سیویلیکا: