Public Key Infrastructures for Trust and Authentication in the IoT

Lavinia NĂSTASE
Faculty of Automatic Control and Computer Science,
University Politehnica of Bucharest, Romania
lavinia.nastase10@yahoo.com

Abstract

The Internet of Things is a global infrastructure of smart electronic devices embedded with sensors with the purpose of collecting, processing, exchanging and delivering data. One of the main requirements of the IoT is that all the connected objects are available at any time. Since the complexity of this network constantly grows, security and privacy are vital for its development. The focus of this paper is on discussing a framework that leverages trust, authentication, encryption and integrity of data, by using a Public Key Infrastructure adapted to the IoT needs.

Index terms: authentication, certificates, encryption, IoT security, PKI, trust models

References:

[1]. F. Hu, "Trust and Trust Models for the IoT" in "Security and privacy in internet of things (IoTs)", CRC Press, vol. 1. 2016.

[2]. J. A. Buchmann, E. Karatsiolis, and A. Wiesmaier, Introduction to Public Key Infrastructures. 2013.

[3]. K. Moriarty, S. Parkinson, A. Rusch, M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, July 2014 [Online] Available: https://tools.ietf.org/html/rfc7292.

[4]. W. Stallings, L. Brown, "Internet Authentication Applications" in "Computer Security – Principles and Practice", third edition, Pearson, 2015, ch. 23, pp. 717–730.

[5]. R. Buyya, A. V. Dastjerdi, "Security and Privacy in the Internet of Things" in "Internet of Things. Principles and Paradigms" in Elsevier, 2016, ch. 10, pp. 183-199.

[6]. M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the internet of things: A survey," Proc. - 2016 Cybersecurity Cyberforensics Conf. 2016, no. August, pp. 28-34, 2016.

[7]. C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos, "Enabling data protection through PKI encryption in IoT m-Health devices," IEEE 12th Int. Conf. Bioinforma. Bioeng. BIBE 2012, no. November, pp. 25-29, 2012.

[8]. Standard X.509 v3 Certificate Extension Reference, [Online] Available: https://access.redhat.com/documentation/en-US/Red_Hat_Certificate_System/8.0/html/Admin_Guide/Standard_X.509_v3_Certificate_Extensions.html.

[9]. M. Benantar, "The Public-Key Infrastructure Approach to Trust Establishment" in "Access control systems: Security, identity management and trust models," Springer, 2006, ch.2, pp. 84-104.