Computer Networks 102 (2016) 83–95

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey paper

On perspective of security and privacy-preserving solutions in the internet of things

Lukas Malina*, Jan Hajny, Radek Fujdiak, Jiri Hosek

Department of Telecommunications, Brno University of Technology, Brno, Czech Republic

ARTICLE INFO

Article history:
Received 14 July 2015
Revised 15 January 2016
Accepted 23 March 2016
Available online 26 March 2016

Keywords:
Cryptography
Internet of things
Performance evaluation
Privacy
Security

ABSTRACT

The Internet of Things (IoT) brings together a large variety of devices of different platforms, computational capacities and functionalities. The network heterogeneity and the ubiquity of IoT devices introduce increased demands on both security and privacy protection. Therefore, the cryptographic mechanisms must be strong enough to meet these increased requirements but, at the same time, they must be efficient enough for the implementation on constrained devices. In this paper, we present a detailed assessment of the performance of the most used cryptographic algorithms on constrained devices that often appear in IoT networks. We evaluate the performance of symmetric primitives, such as block ciphers, hash functions, random number generators, asymmetric primitives, such as digital signature schemes, and privacy-enhancing schemes on various microcontrollers, smart-cards and mobile devices. Furthermore, we provide the analysis of the usability of upcoming schemes, such as the homomorphic encryption schemes, group signatures and attribute-based schemes.

1. Introduction

Nowadays, the Internet of Things (IoT) is a widely-discussed topic among researchers, engineers and technicians. IoT tends to be the next wave of innovation and there are many definitions of the IoT paradigm. For example, IoT can be defined as a highly interconnected network of heterogeneous entities such as tags, sensors, embedded devices, hand-held devices and back-end servers. IoT provides new services and applications that can be deployed in smart homes, transport applications (e.g. Vehicular Ad hoc Networks - VANETs), smart metering, smart grid, etc. Fig. 1 depicts the example of the IoT environment and shows some technologies and appliances that can be used in IoT.

The machine-to-machine and machine-to-human communications are usually based on IP protocol which can cause billions of IoT objects become a part of the Internet. Therefore, the security in IoT has to be addressed due to the high possibility of security risks such as eavesdropping, unauthorized access, data modification, data forgery and unauthorized remote tampering with devices. For example, attackers can turn on smart devices and heating systems to trigger a collapse of the power grid. Furthermore, attacks against routing protocols can be performed in IoT infrastructure and applications, for example, Sybil attacks [1], the sinkhole attack [2].

Security solutions designed for IoT environments have to deal with heterogeneous IoT entities with various hardware specifications. In IoT, the most spread devices are usually resource-constrained devices because of their low cost. These devices usually employ Constrained Application Protocol (CoAP) [3] at the application layer. The security solutions in IoT have to provide the authentication and authorization of IoT nodes (things, users, servers, objects) and data authenticity, confidentiality, integrity and freshness. The security solutions are usually implemented at network, transport and application layers in IoT. Fig. 2 depicts the IoT layers and the security protocols that can be used in IoT, for example, IPSec, Host Identity Protocol(HIP), Transport Layer Security (TLS) protocol, Datagram Transport Layer Security (DTLS) protocol and Slim Extensible Authentication Protocol Over Local Area Networks (SEAPOL). For example, Extensible Authentication Protocol (EAP) messages that ensure Point-to-Point authentication at the link layer can be transfered over SEAPOL or Trust Extension Protocol for Authentication of New deployed Objects and sensors through the Manufacturer (TEPANOM) [4]. Nevertheless, this paper does not aim at the security and authentication protocols at the link and physical layers.

Besides the basic security properties, privacy has to be addressed in IoT as well. Many IoT services and applications provide sensitive and personal information that are exposed, and can be misused by an attacker. Unsecured sensitive data can leak to third

* Corresponding author. Tel.: +420541146963.
E-mail address: malina@feec.vutbr.cz (L. Malina).

http://dx.doi.org/10.1016/j.comnet.2016.03.011
1389-1286/

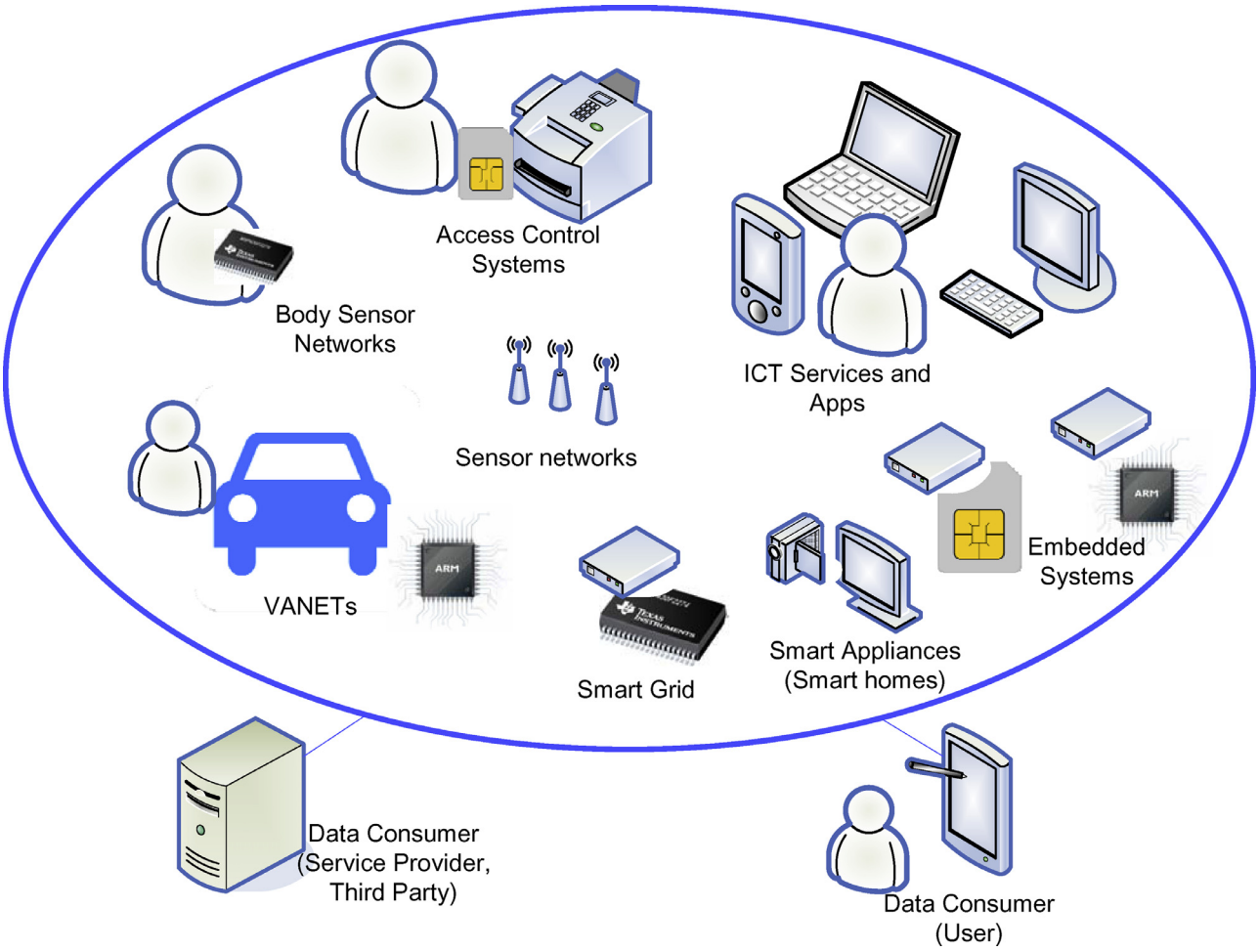

Fig. 1. Technologies and applications in the Internet of Things environment.

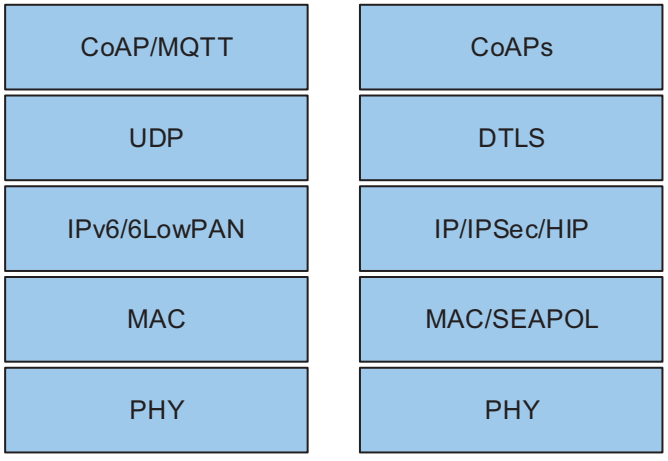

Fig. 2. The Internet of Things layers connected with the security protocols.

parties. The concept of privacy may differ but it should protect user's personally identifiable information and keep a certain degree of anonymity, unlinkability and data secrecy.

A lot of privacy-preserving solutions are designed for powerful computers and nodes in the Internet. The privacy-preserving solutions are usually based on computationally expensive cryptographic primitives, such as bilinear pairing, exponentiation of big numbers. Due to this fact, it is still an open challenge to design a secure, efficient and privacy-preserving solution for the IoT that works mostly with the restricted devices. The main goal of this work is to show how common cryptographic primitives are demanded on various devices and show the perspective of some privacy-preserving techniques in IoT.

This article presents the memory limitations and a performance analysis of cryptographic primitives that are measured on the various devices which are used in IoT. Furthermore, we discuss the applicability and limitations of privacy enhancing protocols and schemes. The main purpose of this paper is to construct specified knowledge in privacy-preserving and cryptographic techniques used in the IoT services. The contribution of this work is twofold:

- We present the performance of widely-used cryptographic primitives on various devices and discuss their memory limitations. We focus mostly on operations which are used in security and cryptographic solutions employed in IoT. We implement and measure these operations on various platforms such as microcontrollers, chip cards and ARM devices.
- We discuss and evaluate the privacy-preserving techniques and schemes in IoT. We implement and measure chosen schemes on various platforms (a chip card, an ARM device, PC). We provide interesting insights about which privacy preserving techniques are better to use in the IoT environment. We believe that this work can help with future research based on privacy-preserving mechanisms in the IoT environment.

The rest of this paper is organized as follows:Section 2 describes an overview of IoT security and presents related works.