Journal Pre-proof

PKI4IoT: Towards Public Key Infrastructure for the Internet of Things

Joel Höglund, Samuel Lindemer, Martin Furuhed, Shahid Raza

PII: S0167-4048(19)30201-9
DOI: https://doi.org/10.1016/j.cose.2019.101658
Reference: COSE 101658

To appear in: *Computers & Security*

Received date: 20 June 2019
Revised date: 3 October 2019
Accepted date: 31 October 2019

Please cite this article as: Joel Höglund, Samuel Lindemer, Martin Furuhed, Shahid Raza, PKI4IoT: Towards Public Key Infrastructure for the Internet of Things, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.101658

PKI4IoT: Towards Public Key Infrastructure for the Internet of Things

Joel Höglund[a], Samuel Lindemer[a], Martin Furuhed[b], Shahid Raza[a]

[a] *RISE Research Institutes of Sweden*
Isafjordsgatan 22, 16440 Kista, Stockholm
[b] *Technology Nexus Secured Business Solutions, Sweden.*
Telefonvägen 26, 12626 Hägersten, Stockholm

Abstract

Public Key Infrastructure is the state-of-the-art credential management solution on the Internet. However, the millions of constrained devices that make of the Internet of Things currently lack a centralized, scalable system for managing keys and identities. Modern PKI is built on a set of protocols which were not designed for constrained environments, and as a result many small, battery-powered IoT devices lack the required computing resources. In this paper, we develop an automated certificate enrollment protocol light enough for highly constrained devices, which provides end-to-end security between certificate authorities (CA) and the recipient IoT devices. We also design a lightweight profile for X.509 digital certificates with CBOR encoding, called *XIOT*. Existing CAs can now issue traditional X.509 to IoT devices. These are converted to and from the XIOT format by edge devices on constrained networks. This procedure preserves the integrity of the original CA signature, so the edge device performing certificate conversion need not be trusted. We implement these protocols within the Contiki embedded operating system and evaluate their performance on an ARM Cortex-M3 platform. Our evaluation demonstrates reductions in energy expenditure and communication latency. The RAM and ROM required to implement these protocols are on par with the other lightweight protocols in Contiki's network stack.

Keywords: security, CBOR, IoT, PKI, digital certificates, enrollment, embedded systems, Contiki

1. Introduction

Public key infrastructure (PKI) is ubiquitous throughtout a wide variety of networked systems for centralized credential management and key distribution. The Internet of Things (IoT) has been slow to adopt PKI due to reasons both economic and technical. Instead, embedded systems often rely on pre-shared keys (PSK), which become problematic when those systems are connected to the Internet and become globally adressable. The keys must be installed before deployment, and because centralized resources must share a key with each device in order to communicate, a single server compromise can put the entire network at risk. Moreover, many basic security guarantees such as proof-of-origin, access control, non-repudiation and authentication are simply not possible with PSK systems.

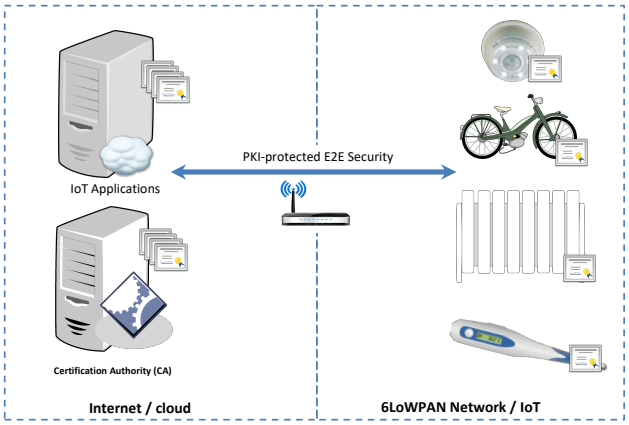

Figure 1: An illustration of PKI-protected IoT setup with end-to-end security between IoT devices and back-end service, without intermediate trusted gateways

Regardless of the simplicity of each individual device, the IoT presents great security risks due to its

Email addresses: joel.hoglund@ri.se (Joel Höglund), samuel.lindemer@ri.se (Samuel Lindemer), martin.furuhed@nexusgroup.com (Martin Furuhed), shahid.raza@ri.se (Shahid Raza)