Mediated Security Pairing for the Internet of Things

Jani Suomalainen

VTT Technical Research Centre of Finland

Received 28 May 2014; Accepted 28 June 2014
Publication 31 August 2014

Abstract

The Internet of Things (IoT) – global connectivity between all kinds of embedded devices and servers – is opening new opportunities for everyday applications. Essential enablers for the IoT are the secure and authenticated connections between things and servers. However, existing solutions for setting up thing-to-server authentication, based e.g. on passwords, trusted certification authorities, or physical connection, are not feasible when servers are far away and things do not have interfaces for inputting passwords or secrets keys. This paper analyses challenges and approaches for security pairing these interface restricted globally distributed things. We explore how mediating devices, such as smartphones, can be used to establish security connections. Particularly, we contribute by analysing how user-friendly security establishment approaches – out-of-band and unauthenticated location-based pairing – can be applied in situations where counterparty is far away or has incompatible interfaces.

Keywords: Internet of Things, embedded device, security, authentication, pairing, mediated protocol, smartphone.

1 Introduction

The Internet of Things (IoT) promises new opportunities for everyday living by allowing all kinds of devices to be connected with other devices and services

doi: 10.13052/jconasense2246-2120.122
© 2014 River Publishers. All rights reserved.