Secure & Zero Touch Device Onboarding

[1]***Dr Mohammad Hossein Zoualfaghari***, *PhD, MEng, MIET* [1*]***Dr Andrew Reeves***, *PhD, MSc* [2]
[1,2]*BT Applied Research, Adastral Park, Ipswich, UK*
**mh.zoualfaghari@bt.com*

Keywords: INTERNET OF THINGS, IoT, SECURITY, ONBOARDING, DEVICE MANGEMENT.

Abstract

As the scale of IoT deployments increase so do the operational challenges associated with physically installing and configuring large numbers of devices in real-world environments. Typical IoT device installation processes have significant manual aspects which drive costs and negatively impact on speed of deployment and security. Here we present the results of a study and prototyping activity which examined the potential for cutting-edge technologies and protocols to automate the onboarding of IoT devices to IoT platforms. This is increasingly being termed secure and zero touch device onboarding within the industry.

1 Introduction

Today, there are over 20 Billion connected devices and the number of devices continues to grow, for example IoT in the manufacturing market growth has a reported growth rate of 29% per annum [1, 2]. When each of these devices is delivered to a customer premise, they need to be installed and manually configured by an expert before being provisioned manually by back office IT staff prior to becoming connected. Then the regular and recursive physical and software maintenance regime can commence, often still with a high requirement for manual interventions [1].

The large number of IoT being deployed makes device management an issue for IoT platform providers. Platform providers have strong incentives to migrate away from current device management processes, which are labour-intensive and time-consuming activities, requiring the individual onboarding of each a device for a new solution or a new customer [3].

Technologies are emerging with the objective of tackling this issue by moving to automated onboarding processes which connect devices with remote management capabilities. This will significantly reduce deployment times, reduce human resources requirements and lower the levels of specialist expertise required to be present at device installations.

2. Methodology

2.1 Challenge definition

The primary technical challenge with the automated remote management of IoT devices is the need to remotely establish the initial trust between the IoT edge device and device management software which forms part of the IoT platform.

Once this initial step is carried out the onward remote management of the device can be carried out in a relatively straightforward manner using well established secure communication methods [4].

This is initial step of confirming that the edge device is in a trusted state is known as attestation and forms part of a secure device onboarding (SDO) process . The challenge which is considered in this paper is how to integrate one of these technologies into an IoT platform architecture which is representative of those deployed by commercial IoT platform providers [5].

2.1 Approach

In collaboration with other major enterprises, a novel edge approach was prototyped with the combined objectives of securely establishing trust remotely, attesting an IoT endpoint and carrying this out in an automated manner [6]. The prototype made use of a commercially available third party onboarding service (Intel® SDO) together with a prototype IoT platform [7].

The solution facilitates a process where when an IoT device is installed and establishes its first connection; it is registered and connected automatically and securely, as a bona fide and fully trusted device, into the cloud-based IoT platform. The platform then adopts the device as a secure device which it begins to monitor and maintain over the air (OTA). This overall process is known as “Zero-Touch Device Onboarding (ZDO)”.

2.1 Cloud Platform Architecture

The cloud platform contains a number of IoT related components which combine to achieve the objective of managing edge devices and making the data generated available to application developers to create their applications to deliver business value. The key architectural components for the current scenario are shown in Figure 1.

2.1.1 Information Exchange

The Information Exchange comprises of a set of services which provided authorised entities with the ability to access data from the IoT devices. Typically the services will include policy controls which restrict which information can be accesses by which user.
Success for the testing activities outlined here was whether a device was able to successfully make its data available within the Information Exchange so that it could be used by applications.

2.1.1 Edge Orchestrator, Container Manager and Device Management

The Edge Orchestrator has a role in ensuring that the edge device is running the software stack defined as most appropriate for that particular device at that point in time. It automates many of the tasks like configuration management, application deployment, and task automation. It works closely with the Container Manager which looks after the compute environment on the edge device. This is necessary as many of the applications and services deployed at the edge are in the form of containerized microservices.

The final standard platform component involved in the prototype was the device management (DM) server. This provides an abstraction layer between the various networking protocols and device protocols to simplify the functionality required by the other platform components.

2.3 Novel components

Building the working prototype required two novel components to be developed within the IoT platform: an attestation server and a bootstrapping server.

2.3.1 Attestation server

The role of the attestation server is to interact with third party solutions, to establish the trust between IoT management servers and remote endpoints. These endpoints will typically come from a variety of individual vendors and their different technologies. There may well also be a number of different 3rd party onboarding services which the attestation service will interact with in order that the goal of being able to securely onboard as wide a portfolio of devices as possible is achieved.

2.3.1 Bootstrapping server

The bootstrapping server automatically prepares and encapsulates the protocols, firmware, applications and device management agents for each device, based on its type, resources, purpose of use and other capabilities. Applications and configurations are then sent to the edge device automatically, using the secure channel established by attestation server. In this manner it is possible to upgrade the device to the latest software stack providing the optimal configuration for the device.

2.3.1 Other key platform components

To facility ZDO the prototype IoT platform also implements a number of newly-introduced and commonly-used IoT standards, such as the Open Mobile Alliance (OMA) Lightweight Machine to Machine (LWM2M) protocol over Constrained Application Protocol (CoAP), on UDP and secured with Datagram Transport Layer Security (DTLS). This eases the integration of the overall ZDO protocol into existing platforms.

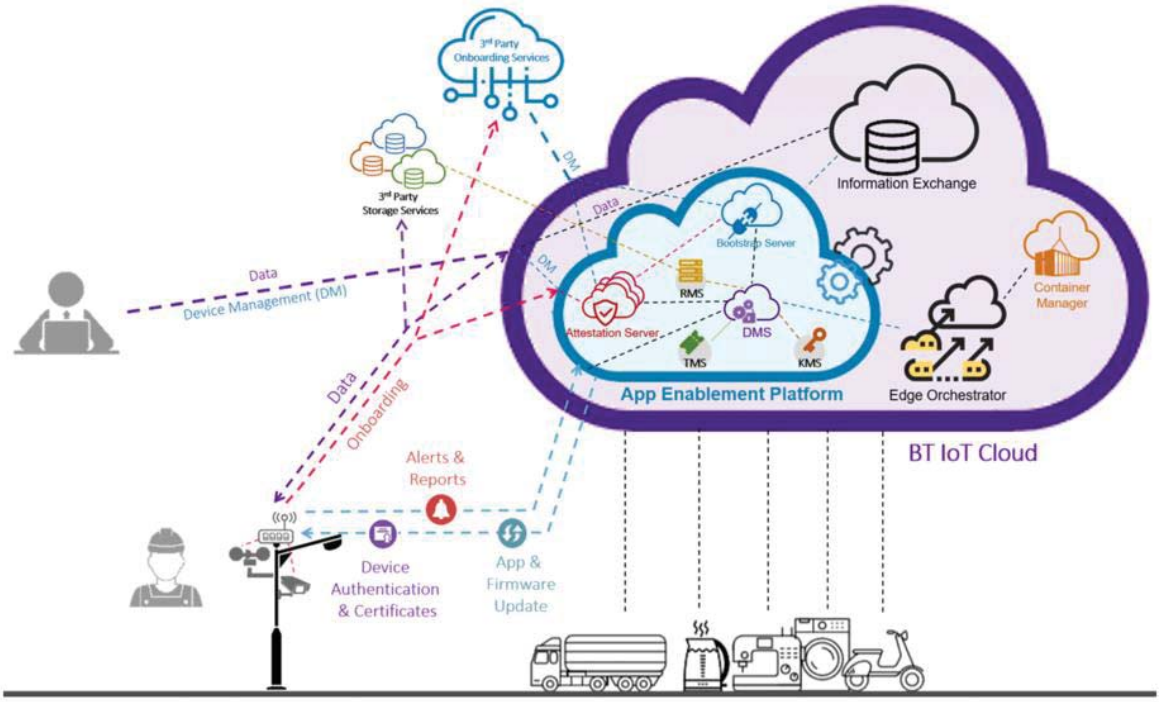

Figure 1: Architectural overview

3 Results

The initial prototype showed that at the first turn on, a device could be automatically attested and receive all the necessary applications and configurations. Testing used raw devices which were turn on and automatically securely configured and started to work as expected, reporting back to the prototype IoT platform.

ZDO was subsequently implemented in a number of further proof of concept (PoC) prototypes, covering the whole life-cycle of an IoT device. This includes: the build process in a manufacturer's factory; shipment to distribution centres; purchase and procurement of the device (physically and digitally); chain of ownership; retailing; arriving at the customer premises; automated provisioning on the first turn on; attestation; bootstrapping (protocols, firmware and applications); automated device management and maintenance over the air (OTA).

The third party onboarding service (Intel® SDO) was available in two different implementations. The first at the physical layer, i.e. using security at the chip level, where the IoT endpoints were Intel® Enhanced Privacy ID (EPID) enabled chips; and also at firmware/software level where EPID was not available on the device. Both approach were tested as part of the prototyping activity.

4 Conclusion

One-by-one and manual onboarding of thousands and millions of devices is a key challenge for IoT providers. Security of these endpoints, which are not necessary powerful in terms of compute power, is also a key challenge for IoT providers. The approach demonstrated showed how cutting-edge technologies and protocols can help to address these issues.

The work also resulted in novel solutions and approaches which allowed SDO technologies to be used in conjunction with IoT platforms to overcome these concerns. This resulted in a number of patents to cover the core platform technology innovations.

To maximise the benefits sought by IoT service providers from ZDO there is a need for widespread adoption across the different hardware manufacturers. Currently, with our collaborators, we are working with industry standard bodies to standardise the protocols and encourage wider adoption.

5 Acknowledgements

The authors would like to acknowledge the close collaboration with Intel® which made this work possible.

6 References

[1] "IoT: number of connected devices worldwide 2012-2025 | Statista." https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed.

[2] TheManufacturer. "IoT in manufacturing market to grow annually by 29%." TheManufacturer. https://www.themanufacturer.com/articles/iot-in-manufacturing-market-to-grow-annually-by-29/ (accessed.

[3] I. Neild, M. ZOUALFAGHARI, T. Stevens, R. Gedge, P. PUTLAND, and B. T. P. L. Company, "Collection of sensor data from sensor devices," 2018. [Online]. Available: https://patents.google.com/patent/WO2018060010A1/en?q=wifi&inventor=zoualfaghari&oq=zoualfaghari+wifi

[4] D. Joshua, D. Gery, Z. Mohammad, B. T. PLC, and B. G. PLC, "Blockchain state reliability determination," 2017. [Online]. Available: https://patents.google.com/patent/GB2549085A/en?q=blockchain&inventor=zoualfaghari&oq=zoualfaghari+blockchain

[5] J. DANIEL, G. Ducatel, M. ZOUALFAGHARI, and B. T. P. L. Company, "Untrusted code distribution," 2017. [Online]. Available: https://patents.google.com/patent/WO2017167549A1/en?q=blockchain&inventor=zoualfaghari&oq=zoualfaghari+blockchain

[6] N. M. Smith, N. Heldt-Sheller, S. Agrawal, M. G. Agerstam, and I. Corp, "System, apparatus and method for transferring ownership of a device from manufacturer to user using an embedded resource," 2016. [Online]. Available: https://patents.google.com/patent/US20160366157A1/en?q=secure&q=device&q=onboarding&assignee=Intel+Corporation

[7] N. M. Smith, R. S. Subramaniam, D. W. Grawrock, and I. Corp, "System, Apparatus And Method For Scalable Internet Of Things (IOT) Device On-Boarding With Quarantine Capabilities," 2017. [Online]. Available: https://patents.google.com/patent/US20170346848A1/en?q=secure&q=device&q=onboarding&assignee=Intel+Corporation