Secure IoT Gateway: Cavium Octeon Tx + MontaVista CGX

Connecting "Things" to the cloud

Secure IoT Gateway Prototype

Table of Contents

Introduction

As IoT device market grows into billions of connected devices, one of the most critical components of future Internet of Things systems may be the "IoT gateway". An IoT gateway aggregates sensor data, translates between sensor protocols, processes sensor data before sending it onward and more.

Fig1: Gateway as a critical device that enables connecting a network of devices to the Application clouds

The importance of IoT gateways is understandable when you consider the explosion in connected "Things" that has occurred over the past few years. With scores of protocols, connectivity models and energy profiles and the highly dispersed nature of IoT systems, gateways are needed to manage and control these complex environments.

Consider the use case of an IoT-connected office building environment. Sensors are the IoT equivalent of our five senses. But instead of five senses, there may be hundreds or thousands of sensors with dozens of different functions, measuring temperature, light, noise, position of people and equipment, particles in the air, building systems operations, security systems, factory machines and more. But IoT is not just about sensing, it's also about controlling systems. Turning on and off lights, HVAC, networks and more can be done through connected systems.

Each of these devices may use different protocols to connect -- such as Wi-Fi, Bluetooth, serial ports (for example, RS-232), Ethernet, MQTT, ZigBee and others. And each of them may connect to different control environments and have different models for management and security.

As the devices, protocols and needs proliferate, having components connect individually back to the systems that need their data is not often possible. Some sensors and controllers use very low energy and don't support energy-intensive protocols like Wi-Fi or Bluetooth, and therefore can't connect directly. Some devices generate so much data that, in aggregate, the data is overwhelming and not all that valuable in its raw form.

This Solution Brief will focus on

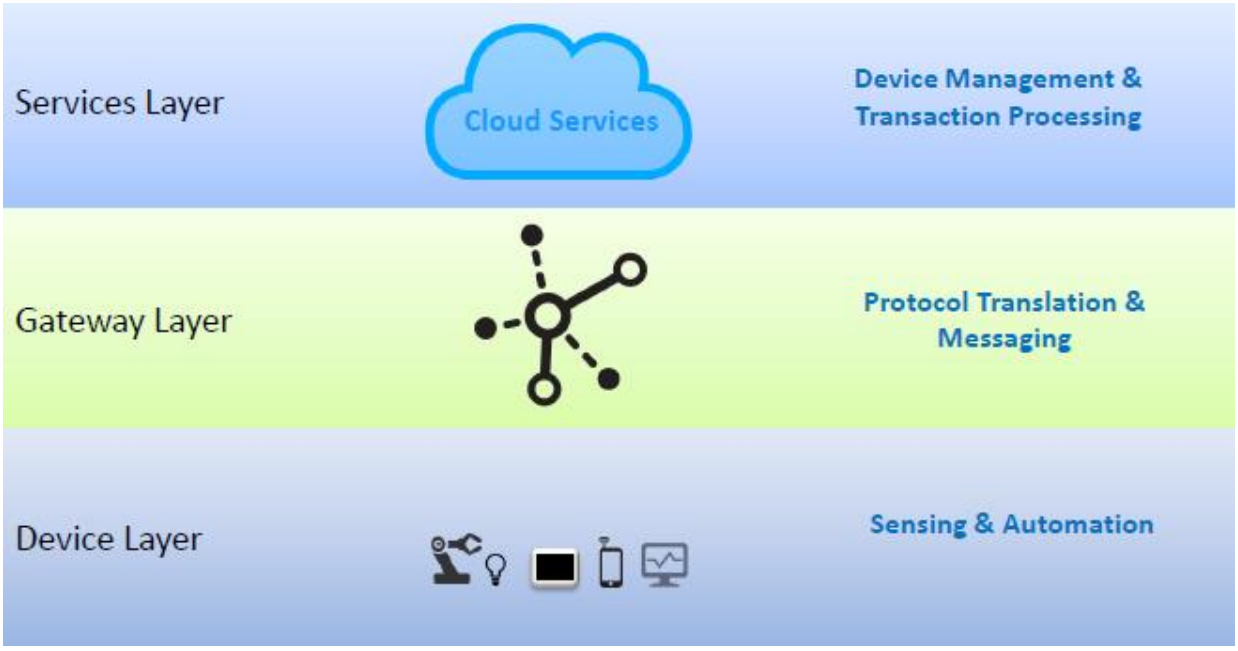
- Purpose, Challenges and Approach for developing Secure Gateways (Edge Computing & Connectivity) in the IoT Architecutre i.e. with Cavium™ Octeon Tx (81xx) based Gateway HW reference and MontaVista CGX (including IoT and Security Profiles)
- Primarily discussion will be on Architecture, Security, and Maintainence features

Note:

- Initial Prototype is being demonstrated in Booth#603 with Cavium Inc. at ARM Tech Con 2016. Dates: October 25-27, 2016. Venue: Santa Clara Convention Center. Location: Santa Clara CA

Developing a prototype for secure IoT Gateway

Understanding an IoT Gateway and the IoT deployment Layers



The simplified IoT model illustrated above shows the gateway layer for the important role of connectivity and messaging between “things”, people, and cloud services. In most cases today, the primary function of the IoT gateway is protocol translation from low power sensor networks to the Internet or LAN.

Sensors, Sensors Everywhere

- Simple sensor data drives the IoT engine

- Fitness trackers, heart monitors, oil and pressure temperature gauges and many more

- What connects them
  - Wireless: Bluetooth, Wi-fi, Cellular Modem, (3G/4G/5G), Zigbee, & 6loPAN
  - The bus lineup: Canbus, Profibus, & Modbus
  - Serial, SPI, I2C
  - Near Field Communication (NFC)
  - Any Prioprietary

To the Cloud

- Data from sensors is the lifeblood of IoT
  - Connects to cloud or database
  - Gateways can filter/preprocess data
  - Push must be secure (encrypted and authenticated)
  - Connectivity is bi-redirectional so IoT Gateway must be secure from the cloud
- IoTivity
  - Community framework to connect end devices
- Alljoyn Open Source Framework
  - Connect and communicate across transports/OSes

Gateway Layer Security

Communications in the IoT usually take place over a combination of private and public networks, so securing the network protocols is obviously important and the first thing you should consider.

Design Consideration

Communications between the things, the gateway, and the cloud service must be cryptographically secured to preserve confidentiality, integrity, and authenticity.

Architectural

- Lifecycle: secure firmware updates and CVEs
    - The Edge is relying on the IT-supported backend to handle the updates, requires careful consideration for the technology and process
- Provide monitoring for end-to-end data on the Gateway
    - Using DPI for heuristics-based detection of exploits
- Combining types of security: physical, networking, system integrity and isolation of domains

Functional

- Building security primarily in the Gateway?
    - Edge devices are constrained on hardened channel
    - Requires encryption for the channel and two-way authentication for setup
- Trusted edge vs. Edge Computing - two polars?
    - Moving computing to the edge can help build end-to-end efficiency, but requires edge and gateway devices to handle the security

- Can also be seen as a way to fence out security threats for some layers of the processing so they cannot be exploited from the Cloud

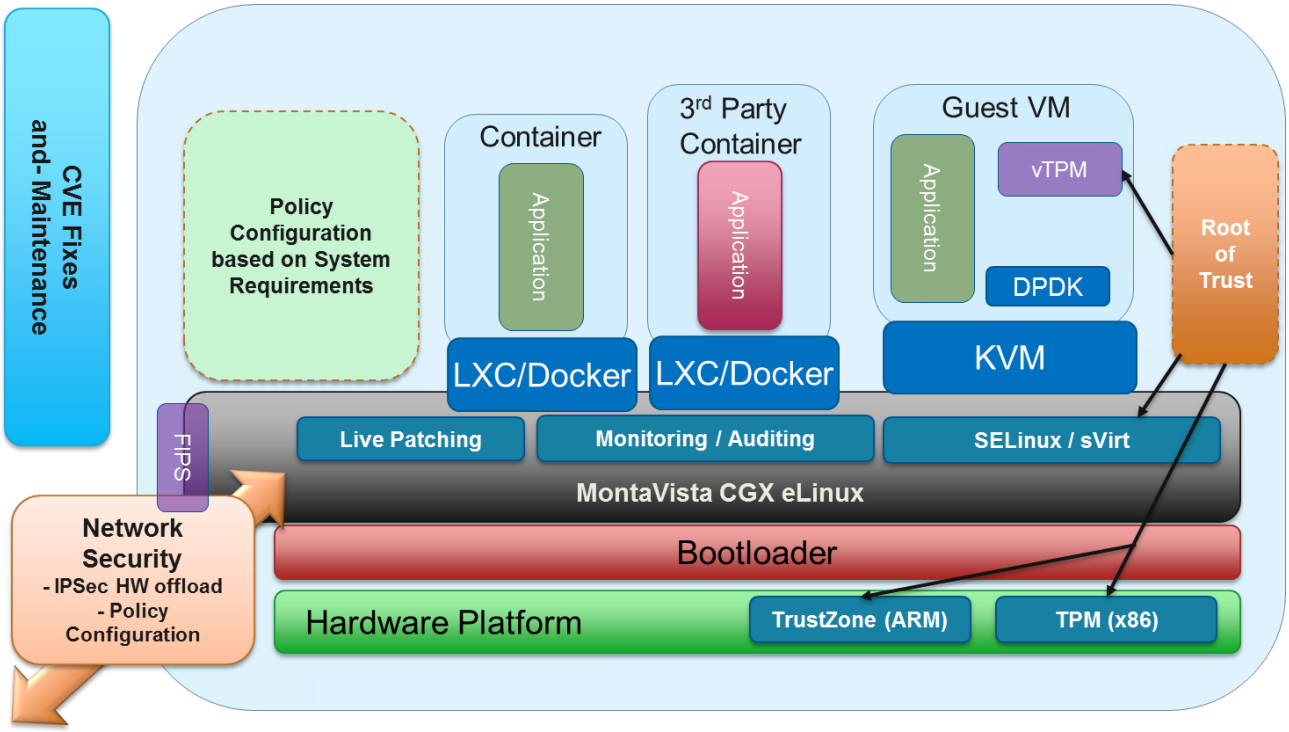


Fig: IoT Platform Virtualization Block Diagram

Securing network communications in this way, with technology like AES cipher suites and TLS/SSL encryption, is probably the most understood area of IoT security since we've been doing it for years for applications like e-commerce over the Internet.

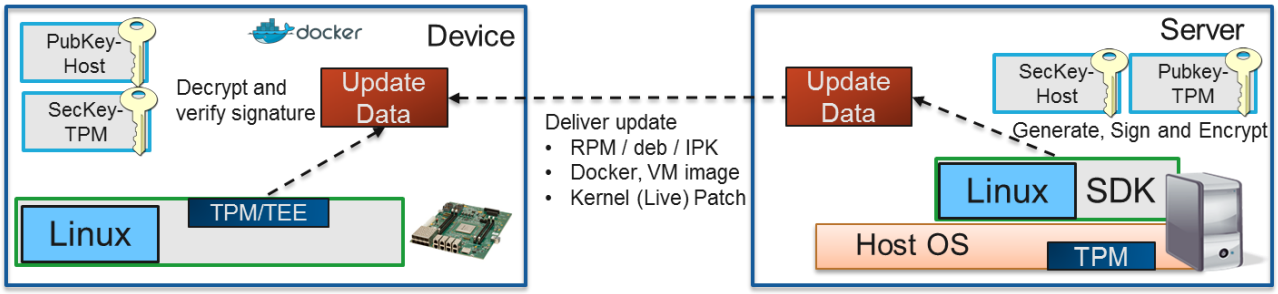
End-to-end Encryption

If an attacker were to compromise the IoT gateway, not only the data passing through the gateway is at risk, but control of the physical things connected to it are at risk as well. **One way to mitigate this problem is to implement true end-to-end, application layer security.** Using this strategy, messages are encrypted in a way that allows only the unique recipient of the message to decrypt it, and not anyone in-between.

The Allseen Alliance AllJoyn IoT standard is maturing nicely and has great documentation on how they are approaching secure onboarding and cryptographic security in their ecosystem.

Firmware Updates

Since many IoT devices gateway don't have much in the way of UI or internal storage, an external application and gateway is often required to retrieve and apply firmware updates. To update firmware securely, the system should record current version and new version of the firmware, check for a valid signature on the downloaded firmware upon receipt, and check firmware integrity before firmware installation.



IoT devices and Gateways have embedded requirements for small footprint but still a very high demand for security

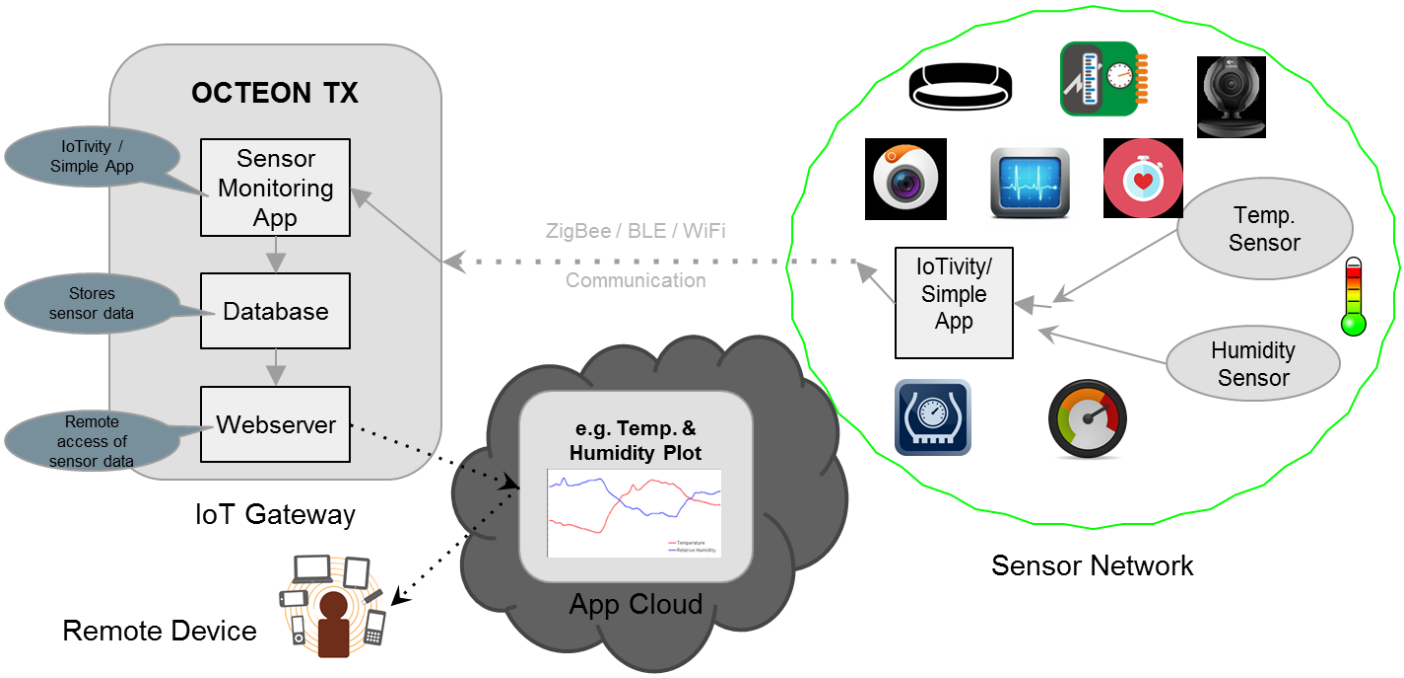
The process relies on the Kernel Live Patches, RPMs, or Container images being hashed and signed by a certificate that can be validated by the TPM or TEE on the target system if necessary. Can also support two-way signatures by using standard RPM signing using GPG keys, potentially enforced by the server-side TPM.

Such processes are adopted by OSVs like Symantec, Redbend and practically all product manufacturers that are concerned about running trusted/secure SW on the devices.

Without secure updates, the integrity of the platform cannot be maintained.

Prototype IoT Gateway

To fill the need for a secure IoT gateway for the enterprise, we have tried to provide a prototype/ Proof of concept design that is designed to integrate protocols for networking, embedded control, security and manageability and provides a platform on which 3rd party applications can run.



Related Products and Services

MontaVista Carrier Grade eXpress®

MontaVista® Linux® Carrier Grade eXpress (CGX), delivers Carrier Grade reliability, security, and serviceability that is highly configurable, flexible, and of consistent high quality. CGX meets the demands of the interconnected intelligent devices, providing application portability, dynamic configuration, field maintenance, and real-time performance in a single platform.

CGX will address a very large embedded device segment including networking and communications, instrumentation and control, aerospace and defense, SOHO devices, medical electronics and the "Internet of Things (IoT)" markets.

For more information, http://mvista.com/product-cgx.html

MontaVista Professional Services

With over 15+ years of commercial Linux experience in helping our customer develop embedded device, MontaVista offers an unmatched mixture of skill and experience to ensure success. Offering highest flexibility of both time and scope, customers can leverage MontaVista expertise through the development and deployment process.

Our services value proposition consists of –

- In-depth Linux expertise,
- Standard up-front pricing options,
- Clear and predictable engagement process,
- Flexibility and Scalability, with
- Our global presence
- Always On-Time, On Budget

Since 1999, MontaVista has been a leader in embedded Linux commercialization, helping our customer successfully deploy 100s of millions devices till date and counting.

For more information, http://mvista.com/product-proservices.html

Summary

The primary role of the IoT gateway is connecting low power sensor networks to private Ethernet LANs and to the Internet. As the number of devices proliferates in the enterprise, the role of the gateway will grow to handle the increased network traffic and include functionality like local processing of device automation, device management, and network access policies. It's not hard to see that the gateway plays a vital role in the IoT, but to be included in the enterprise, it must be secure.

MontaVista can assist at every level of development, deployment and on-going maintenance and support of your final product.

http://www.mvista.com/contactus.php

MontaVista HQ, San Jose, CA

MontaVista Software, LLC 2315 North 1st Street, 4th Floor
San Jose, CA, 95131

Tel: (408) 943-4500