wolfBoot for Secure Startup

Aloxy delivers reliable, industrial IoT solutions specific to the (petro)chemical and oil & gas industry. The Antwerp-based company has grown quickly since 2017 and combines expertise in valve maintenance, process safety and efficiency, and software development to enable high-performing, data-driven applications and sensors for IoT.

Key Requirements

The stakes are high in Industrial IoT. Sensing equipment must be robust, secure, and certified for explosion safety. Maintenance in the field can be very expensive in this safety critical environment, requiring different types of approvals and an extensive process.

For this reason, Over-the-Air (OTA) updates are a great option for use cases such as Aloxy's, enabling security and algorithm updates on sensors which remain in the field for 5 to 10 years. The *Aloxy Pulse* sensors are used to track the position of manual valves on site. The sensor measurements are transmitted wirelessly to gateway infrastructure and processed on the back-end IIoT platform.

"Having a secure boot is very important for an IoT device. For a small start-up, as we are, it doesn't make sense to roll your own boot loader, especially since this is security sensitive. It makes more sense to buy a commercially available boot loader which is open source."

The main question for Aloxy was how to achieve firmware updates and secure boot.

"Daniele did a great job of assisting [our implementation]. He was very responsive, with expert support."

Solution

After looking at several other options for secure boot, including one that was strictly open source, Aloxy found that wolfBoot was the easiest to get started, and the team was encouraged by the option for commercial support.

wolfBoot's minimalist design, portability and OS-agnosticism made it an easy fit for Aloxy's target, which was STM32L0 hardware with a lightweight operating system and OSS-7, a fully open source DASH7 implementation.

wolfBoot already had support for Aloxy's target environment, so getting started was a breeze.

Results

With clear and informative documentation and a responsive team of engineers, wolfSSL was able to support Aloxy's secure boot implementation in *Aloxy Pulse.*

The key components to this solution's feasibility were easy integration to provide firmware update mechanisms, made possible by wolfBoot's minimalist design and tiny HAL API.

wolfBoot supports multiple keystores and/or hardware-based public-key accelerators, such as Freescale-LTE and STM32-PKA. TPM-2.0 support is provided through the integration with wolfTPM.

"Our commercial solution enables wolfSSL [technology] to continue to enhance its usage, for growth and reuse on other [Aloxy] targets."

Aloxy is currently focused on the firmware update functionality from wolfBoot, but the team is looking into wolfTPM usage for connecting secure elements in future designs.

For More Information

wolfSSL prides itself on providing a GPLv2-licensed version of wolfSSL in addition to commercially-licensed versions, with the GPLv2 version available direct from our website. With the GPLv2 download, companies like Aloxy can test and prototype before making a license decision.

www.wolfSSL.com   facts@wolfSSL.com   @wolfSSL
www.aloxy.io   info@aloxy.io   @Aloxy_io

This document is intended for informational purposes only.A wolfSSL Inc. makes no warranties, express or implied, in this document.

*Other names and brands may be claimed as the property of others.