ETSI The Standards People

IoT Conference 2023

Streamlining Device Security

A Case Study in Meeting Evolving IoT Security Demands

Presented by: KAUSTABH DEBBARMAN

LAAVAT

05/07/2023

“It takes 20 years to build a reputation and a few minutes of a cyber-incident to ruin it”

Vaisala, a global leader in weather, environmental, and industrial measurement solutions

Why is IoT security important?

For manufacturers of machinery control components such as controllers and embedded IoT gateways and sensors

Without appropriate controls, device manufacturers are at risk of loss of critical intellectual property, credibility, and brand damage, and are subject to liability risks.

Need to conform to evolving legislation, standards such as IEC 62443, and customer mandates for IoT security.

What device manufacturers need to keep in mind

When developing and deploying their products

IoT devices may need to be supported for a long time

Portfolio usually has multiple devices based on different MCUs from different silicon vendors

A secure software supply chain is the foundation of secure IoT devices

VAISALA

A leading provider of weather, environmental, and industrial measurement solutions

Photo credit: Vaisala

Why is IoT security important for VAISALA

"Weather data is essential for critical functions in society. As a leader in weather, environmental, and industrial measurement technologies, our customers count on us to ensure reliable and trustworthy data.

Product and software security is the foundation of the data we enable for our connected world"

Photo credit: Vaisala

Vaisala's security platform prevailed against cyberattacks from 100 hackers in Nokia Security HackAthon 2020

For Vaisala's customers, it's not that much about confidentiality, but data integrity and authenticity is what matters when peoples' lives are at stake – or the planet's future

What does a secure IoT device mean for VAISALA customers

Unauthorized access is prevented

Running unauthorized software is prevented

All communication is encrypted and secured

A strong and unique device identity

Secure software update capability

Protecting VAISALA devices and data from unauthorized usage, manipulation, and control

An approach based on mainstream security technologies

Centralized cryptographic key management for effective use of cryptography for operations such as digital signing and encryption

Digital signing and packaging of software releases to ensure that the device firmware updates always come from a trusted source

Encryption of firmware images to ensure protection of Vaisala intellectual property in the IoT device software.

Protecting VAISALA devices and data from unauthorized usage, manipulation, and control

An approach based on mainstream security technologies

Secure delivery and programming of cryptographic keys and the issuance of unique initial device identities during manufacturing to prevent malicious activities such as the creation of cloned and counterfeit products

Usage of Public Key infrastructure-based solutions to enable secure device management based on mutual authentication and encrypted communication

Lessons learned from VAISALA

IoT devices need to be supported for a long time

Business continuity of the security solution in use

Proper key management with well-defined key ownership

Lessons learnt from VAISALA

A device manufacturer may have multiple devices based on different MCUs from different silicon vendors

Uniform way to manage cryptographic artifacts and operations for IoT devices based on most widely used MCUs

Lessons learnt from VAISALA

Secure software supply chain is the foundation of secure IoT devices

Utilisation of trusted mainstream components for embedded security feature development

Cryptographic operations such as digital signing and encryption are controlled

Secure distribution and provisioning of cryptographic artifacts

About LAAVAT

Device manufacturers use our solution to enable embedded security features, including secure boot, secure firmware update, protection of critical IP, and strong device identity for devices based on various MCUs

World-class expertise in cryptography, embedded development, building and managing business-critical security solutions

A strong heritage of expertise in securing hundreds of millions of smart devices from Nokia, Microsoft, and Intel

AWS Certified Solution architects, CISSP's

ISO 27001 certified

British
Assessment
Bureau
UKAS
MANAGEMENT
SYSTEMS
8289
ISO 27001
INFORMATION SECURITY
MANAGEMENT

Thank you

Accelerate the creation of secure IoT devices

Ensure compliance and business continuity

laavat.com