Press Release
Lee O'Toole
Marketing & Communications
L.OToole@andersdx.com

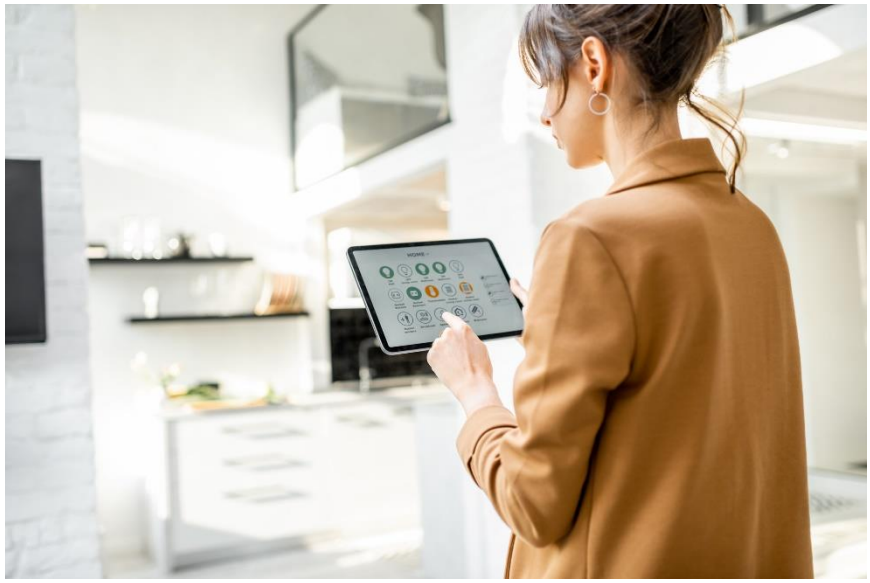
Anders Tell Us About i.MX 8 Security
How Can IoT Devices be Properly Protected Against Cyber Threats?

By Liem Tran, Applications & Development Engineer, Anders.

The IoT is no longer a novelty and is now the basic enabler for smart living and backbone for enterprise digital transformation. Keeping hackers out is a priority and the latest generations of chips and boards are equipped to meet emerging security standards for connected "things".

How are Approaches to Securing IoT Edge Devices Changing?

We are all familiar with the phrase, "Security is only as strong as the weakest link." When it comes to the IoT, there can be a huge number of links to think about. It's reckoned that about one million new devices are added to the IoT every day.



Devices connected to the IoT, like smart sensors, thermostats, door-entry controllers, are usually designed within strict limits on processing capability and power consumption. There is little computing performance, if any, to spare for running intricate security software.

Moreover, cumbersome security would hamper interactions with the device and compromise the performance of the application. In any case, hackers can often bypass software-based security like passwords.

As the requirement for proper IoT security has become recognised, effective techniques and policies for securing edge devices - embedded, remote, and often autonomous connected "things" - have become standardised. This helps device designers, installers, and operators implement security measures that are adequate for the type of device and the likely cyber threats it will face when deployed. Hardware-based security features that support these standardised approaches and hence enable recognised levels of assurance are now built into IoT devices ranging from the simplest microcontrollers to sophisticated computer modules.

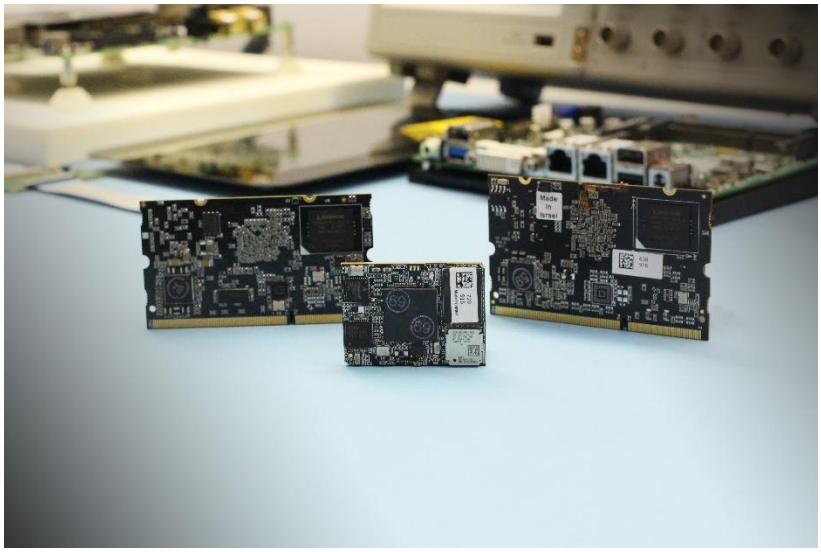
We can see evidence of this toughening stance on cyber security in application processors like NXP's i.MX 8 family, as well as computer modules from companies such as CompuLab that combine the processor's built-in security with additional on-board features to raise the level of protection for equipment like gateways.

What Security Threats does Equipment Built with i.MX 8 Boards Typically Face?

Depending on the type of device, cyber attackers may be trying to steal information such as personal data, intellectual property, or passwords. Alternatively, they may be aiming to take over and use devices to cause harm to their owners/operators or to attack other targets – such as by organising them into botnets or swarms to launch DDoS attacks or send spam. Devices equipped with cameras or microphones may be used for spying. Ransomware attackers may simply disable devices and demand payment to restore their functionality.

Preventing these sorts of attacks requires mechanisms to ensure that only authorised software is programmed into IoT devices when new. Moreover, the software's authenticity needs to be verified each time before boot-up and unauthorised attempts to change the software need to be blocked. Application code and data stored on the device or exchanged with others such as a gateway device usually needs to be encrypted to prevent interception.

How can Small IoT Devices Resist Cyber Attacks?



The i.MX 8 family processors come equipped to handle cyber threats, with Arm® TrustZone® technology that provides hardware-based isolation of security-critical processes and data to create a root of trust within the device. TrustZone includes various options for SoC designers to meet specifications established by security bodies like GlobalPlatform and PSA.

Other i.MX 8 security features include the Cryptographic Accelerator and Assurance Module (CAAM), which provides hardware-enforced access control for secure memory as well as cryptographic authentication, encryption using the latest algorithms, handling of symmetric key ciphers, and random number generation.

System boot-up is one of the times when IoT devices are particularly vulnerable to attack. i.MX 8 processors feature NXP's High-Assurance Boot (HAB), which checks the application code's digital signature for authenticity before being allowed to run. Look out for our upcoming security-related posts that will describe secure boot and cryptography, examining their roles in the authentication chain and in establishing the root of trust.

How do Board-Level Security Features Work with the i.MX 8 Security?

CompuLab has integrated a Trusted Platform Module (TPM 2.0) on the IOT-GATE-iMX8 board, which contains its own secure CPU and secure storage. It can work in conjunction with the i.MX 8 processor's security features to provide services such as secure storage of software measurements taken to ensure authenticity. These measurements, protected inside the TPM against tampering, can support remote attestation of the device as well as identify and restrict access for rogue software.

What is the Role of Software in Protecting IoT Devices?

Proper security for embedded hardware also requires closing all doors such as debugging ports, which can provide a gateway for malicious attacks. We will focus on this and other techniques for ensuring resistance to physical attacks in an upcoming blog.

Of course, hardware features alone do not constitute a complete security strategy. Hardware provides the immutability needed to establish trust in a device, while software-based security measures are needed to interact with the hardware and provide overall control for processes like secure boot and installing updates. For this, i.MX 8 developers can leverage a well-developed interface with Mender, a platform for remote device management. Mender, which comprises client software, centralised management, and a web user interface, helps distribute updates to devices in the field. It ensures security as well as providing features to manage large fleets of devices including configuration, customisation, and troubleshooting. Stay tuned for more on network security and resisting cyber-attacks in a future post.

Our embedded design specialists can help you make the most of the hardware-based security available with i.MX 8 processors and boards and develop the security software to manage your devices securely and efficiently. To find out more about keeping your devices safe on the IoT, contact us today.

About Anders

Anders Electronics. is the market leader for solutions in display, embedded, and LED technology.

From design to development through to the supply of world class products for global B2B customers, they are the engineering and industry specialists, dedicated to making electronic touchscreen technology engaging and enjoyable.

Over 30 years ago, Anders started designing, developing, and delivering customised display solutions for the non-consumer industry and they haven't stopped innovating since! Anders features a history of reliability and innovation, and lives to solve display engineering challenges.

Anders harnesses their expertise in display, embedded computing and touch control technology to help differentiate their customers' products through exceptional design and engineering.

With an unrivalled depth of service, scope of engineering skill, scale of capabilities, global manufacturing reach, and speed of operations, the Anders portfolio is the most comprehensive in the industry.

Anders, the people behind the screen.

For further information, please visit our website at https://www.andersdx.com/.

YouTube: https://www.youtube.com/channel/UC5Oc0xqNkHLDdcTHZ2u3UXw
LinkedIn: https://www.linkedin.com/company/anders-electronics/
Twitter: https://twitter.com/AndersElec