INTERNET OF THINGS

Security Solution Checklist

To protect against ever-increasing ecosystem intrusions (access breaches), IoT device makers must build products that protect and secure the network connections with which their devices communicate to servers, databases and other services.

Verification and authentication are key in this effort and must be done mutually to ensure a higher level of communication security. For every communication link established between two communicating nodes,

YOU MUST BE ABLE TO VERIFY:

The identity of the device & the identity of the server.

Ideally, in a full, more advanced implementation, you should also use authentication to verify the signature of any code executed by devices in your ecosystem.

Follow this checklist to make sure your products accomplish these critical objectives.

ENCRYPTION DOES NOT EQUAL SECURITY.

A common misperception is that cybersecurity is about data encryption. Encryption is necessary but not sufficient. Good cybersecurity practices incorporate strong identity authentication as their basis.

UNIQUE DEVICE IDENTITY.

Security solutions must create a unique, verifiable identity (authentication) for the device, allowing you to enforce access control on a very granular level if needed.

REDUCE THE RISK OF NON-ADOPTION.

To increase the chances for adoption, you need a solution that fits seamlessly into your existing manufacturing flow for hardware devices.

PROVIDE MULTIPLE LAYERS OF PROTECTION.

Look for a solution that uses strong, identity-based authentication model (preferably certificate-based). A security solution that relies on a traditional username and password model should be a huge red flag.

THINK SECURITY FIRST.

Introducing your security in the design stage allows you to incorporate it into your overall solution architecture and your manufacturing flow.

AIM FOR ECONOMY IN COST AND TIME.

Choose a security solution provider that understands hardware manufacturing to keep bill of materials (BOM) and development time costs in check.

SECURE UPDATES.

Many security issues occur because manufacturers know they need to update their devices but don't know how to do it properly. If a device can't be securely updated after deployment, it will be highly vulnerable to large-scale malicious attacks.

SIMPLIFY THE IMPLEMENTATION SOLUTION.

Working with a security solution provider that understands the hardware manufacturing supply chain can make implementing security much more seamless.

PKI-based security originated as an enterprise computing solution, but proper design philosophy and adaptation to hardware manufacturing logistics allows it to be scalably applied in individual IoT devices.

Visit us at www.kyrio.com or email us at info@kyrio.com

KYRIO™