Security Frameworks to Set the IoT and IIoT in Motion

Posted by: DE Guest in Commentary, Internet of Things June 1, 2016

By Oliver Winzenried, founder and CEO, Wibu-Systems

Security has become a prime concern for manufacturers of IoT (Internet of Things) devices. It is indispensable for using the devices as they were intended, upgrading them without exposing them to tampering and monetizing features in new business models that benefit device makers and users alike.

Current devices often remain standalone and proprietary solutions with unchanging functions. Revenues are often associated with the original sale, and streams of income from maintenance are unpredictable. However, new devices are becoming upgradable with features sold on marketplaces akin to app stores, turning one-time sales into recurring revenue schemes.

Security Vulnerabilities in the IoT

As software has taken the prime position, a new generation of attackers is born. They may come from organized crime, terrorism, secret services or industrial competitors; have virtually unlimited resources for highly sophisticated attacks; and are determined to exploit loopholes in software, firmware or archiving systems. They counterfeit software to run on other devices, reverse-engineer algorithms, unlock functions, manipulate systems with tampered firmware or entire fake identities, or plunder sensitive data of manufacturers, their customers and end users alike. In an era of increasing cybercrime, IP (intellectual property) and tamper protection need uncompromising security.

Security Solutions in the IoT

This is not the time to oppose the inevitable transformation or sit on the fence. The market offers a number of solutions to prevent IoT attacks and embrace the industrial revolution.

1. Know-How Protection: The actual assets — the IP in the code — are encrypted with lightweight symmetric encryption and only decrypted on the fly.

2. Product Protection: Counterfeit products cannot be made without decrypting the data, possible only on licensed machines.

3. Flexible Licensing: Allows options like pay-per-use, renting, subscription etc. for software features. Vendors decide how licenses are deployed, either in app stores or user license portals.

4. Tamper Protection: Application code is digitally signed using asymmetric cryptography, with root public keys as securely stored anchors of trust. The devices validate authenticity and integrity themselves.

5. Device Identity: Connected devices need to authenticate themselves, e.g. with tamper-proof private keys. Open standards like OPC UA are excellent solutions for trusted devices of different makes to operate together.

Alongside top-notch encryption mechanisms, the strongest approach to security relies on secure elements: Hardware components that can be added to a machine or device and that hold the cryptographic keys and the software licenses safely locked. These elements can include dongles, memory cards, Trusted Platform Modules and ASICs (application-specific integrated circuits). In ruggedized environments — subject to extreme temperature, vibration or humidity fluctuations — the selection of secure elements, designed with industrial-grade components able to withstand harsh conditions and operate reliably, is paramount.

There is a plethora of platforms currently supporting manufacturing processes. Their storage and computational capacities are decreasing down the line from industrial computers, to embedded systems, to PLCs and microcontrollers. The core security functions can still be enforced in all of these devices. Security systems and best practices can be applied to new facilities as well as retrofitted existing plants.

Rethinking the Business Model for IoT

IoT devices are connected to the internet to allow for constant tweaks to the entire system. The real-time analysis of Big Data can provide tremendous insights for predictive maintenance, sales models or performance optimization. Whether it's a security patch or a new feature that is being injected over the cloud, IoT introduces dynamic patterns into the game. The entitlement to software updates, upgrades and new functionalities can best be delivered when the complete license lifecycle management is integrated with ERP, CRM and e-commerce platforms.

The integrity of IoT devices can be ensured with cryptographic processes and secure hardware. Properly implemented, such encryption can pave the way for all-new business models.

Oliver Winzenried is the founder and CEO of Wibu-Systems, a digital rights management company. He is also chairman of the "Protect-Ing" working group of VDMA, on the board of directors of BITKOM and the Research Center FZI at the Karlsruhe Institute of Technology, and is a member of the Industrial Internet Consortium, IIC. Send e-mail about this commentary to DE-Editors@deskeng.com.

Tagged with: CYBERSECURITY INTERNET OF THINGS WIBU-SYSTEMS