White Paper Executive Summary

Integrity Protection for Embedded Systems

Balancing Security with the Benefits of Industry 4.0

With the emergence of Industry 4.0, control systems are becoming increasingly interconnected and communicating over public networks. The added value brought by these systems operating in unison in the IoT and Industrial IoT has been proven beyond all doubt in recent years. However, public networks greatly expand the attack surface for cybercriminals trying to take advantage of the many vulnerabilities that can be exploited.

At the heart of these controllers stands the embedded software that must be protected to not only prevent the loss of intellectual property, but also the introduction of malware through malicious code tampering – in other words: Guarantee the integrity of the system.

Integrity protection encompasses security measures that safeguard system resources, programs, and data against unauthorized manipulation. The main challenge is to guarantee data integrity, bring the system into a safe mode, and stop the execution of all functions as soon as an attack has been detected. The integrity of embedded systems can be ensured by using cryptographic methods in a clearly defined process and relying on a secure hardware device for key management and state storage.

This white paper describes the basic tenets of integrity protection, identifies key attack points to cyber-physical systems, defines the basic measures at work behind the encryption mechanisms, and addresses the many challenges involved in protecting embedded systems. It illustrates the basic configuration of an embedded system and its protection with Wibu-Systems' CodeMeter smart card-based technology.

The white paper also explains the steps involved with CodeMeter's implementation of the integrity check:

- Creating an OEM software version
- Encrypting the program code to prevent static code analysis and reverse engineering
- Signing the program code of both the application and operating system image
- Storing the public elements needed for the decryption process
- Storing the private signature key on the vendor's site
- Implementing signature and hash verifications during loading and runtime operations

The white paper also reviews additional protection measures, including backward checks, boot loaders, and chains of certificates

CodeMeter supports all popular operating systems like Windows, macOS, or Linux as well as Windows Embedded, Real-Time Linux, VxWorks, and PLCs like CODESYS and others. It contains a secure implementation of symmetric and asymmetric encryption methods (AES, RSA, ECC) as well as hash functions (SHA-256), functions for signature validation (ECDSA), and a random number generator. CodeMeter comes with all the available tools needed to implement the toughest integrity and software protections and safeguards against code tampering in the market.

5062-015-02/20190821

sales@wibu.com | www.wibu.com

WIBU SYSTEMS