White Paper
Intel® Trusted Execution Technology and Intel® Virtualization Technology
Design House and Platform Solutions

Securing and Consolidating Industrial Automation Systems Based on Intel® Architecture Using Open Source Technology

Using open source components, Intel demonstrates how Intel® Trusted Execution Technology and Intel® Virtualization Technology complement existing security measures for networked industrial systems based on Intel® Architecture.

Executive Summary

This paper presents an overview of the importance of security for today's connected industrial automation systems and highlights the benefits of Intel® Trusted Execution Technology (Intel® TXT) and Intel® Virtualization Technology (Intel® VT) in complementing existing security measures. Furthermore, a demonstration system (a product separation industrial machine) using open source technology is described with a procedure that may be considered to set up the system.

"This demonstration of a security solution for industrial automation systems uses open source technology with Intel® Architecture. By designing security into its processors, Intel ensures security is inherent in deployed systems based on Intel® Architecture with Intel® vPro™ technology."

Yau, Wai Yeong
Intel Corporation

Lee, Zhan Qiang
Intel Corporation

Background

Industrial automation systems are increasingly connected to each other in a manufacturing environment as part of the Internet of Things (IoT) concept where real-time information from connected devices can be consolidated, analyzed, and acted upon. This connected approach to manufacturing is not limited to a single site; the approach has evolved to a site communicating with other sites, enabling decision-making at a higher-level by connecting the information from the device level to enterprise resource planning (ERP) systems at the enterprise level.

With the rise of connected devices in the manufacturing environment, the focus is now on security and consolidation. Unlike conventional closed systems, today's connected industrial automation systems are susceptible to cyber threats, such as zero-day rootkits. These threats, if detected at all, exploit previously unknown security vulnerabilities in the operating system and application software in order to access confidential data or to manipulate processes in connected systems. The potential consequences of a security breach on connected systems may include loss of productivity, harm to corporate reputation, and damage to equipment.

Securing industrial automation systems requires a comprehensive solution with multiple layers of security measures without impacting performance or limiting accessibility. One of the layers is Intel® TXT, which provides security at the hardware level even before the operating system is running to ensure a trusted computing base. After the operating system loads uncorrupted, protection is then provided by other security layers, such as an antivirus software that detects runtime viruses and a security policy that compartmentalizes applications and the system where access is restricted to specific users.

Table of Contents

Ensuring Trust with a Hardware-Based Security Foundation

The computing infrastructure of an industrial automation system only offers protection — for example, through the installation of third-party security software and the implementation of security policies — after the operating system loads. The challenge is ensuring the operating system can be trusted before it loads.

Establishing a Measured and Verified Boot

The 4th generation Intel® Core™ processor with Intel® vPro™ technology[1] offers integrated hardware support for intelligent management functions, virtualization, and platform security. To complement existing security measures that ensure trust in the computing infrastructure of industrial automation systems, the combination of the Intel® Core™ vPro™ processor, chipset, the Trusted Platform Module (TPM), and firmware compose Intel® Trusted Execution Technology (Intel® TXT). Intel® TXT is a hardware-based security foundation that provides a trusted starting point for the operating system, prevents unauthorized software, and enforces trusted configurations.

Before the operating system is launched, restarted, or resumed from sleep, Intel® TXT establishes a trusted computing platform by ensuring the launch environment (such as BIOS and virtual machine managers) is secure by measuring critical elements in comparison with a known good source and verifying the launch components using cryptographically generated digital signatures. Therefore when the operating system is running, it is running on a trusted computing platform. However, the computing platform still requires security measures against runtime threats and malicious intentions via third-party solutions.

Consolidating Workload and Enhancing Control

The 4th generation Intel® Core™ vPro™ processor supports hardware-based virtualization in the form of Intel® VT[2], which increases the robustness of the virtualized environment by ensuring virtual machines do not interfere with each other and accelerates data transfers by directly and securely assigning I/O devices to the guest operating systems.

The separation of software from hardware in virtualization allows several operating systems to run on a single computing platform, with individual virtual machines managed by a hypervisor or a virtual machine monitor (VMM). The hypervisor abstracts the hardware requirements for software, so each virtual machine appears to run on its own computing platform.

This consolidation of computing infrastructure for industrial automation systems allows greater flexibility when it comes to enhancing security. Consolidating the computing infrastructure results in fewer computing platforms that require security solutions. Fewer computing platforms also reduces the points of attack by unauthorized users.

Simplifying the efforts towards these goals is the Intel® Industrial Solutions System Consolidation Series, which is a solution that includes the essential hardware and software. A demonstration of using this solution with a commercial security software is detailed in the solution brief at http://www.intel.com/content/www/us/en/industrial-automation/mcafee-how-to-secure-manage-industrial-systems-brief.html.

However, the demonstration presented in this paper uses open source components to enable the security and consolidation of the computing

platform in an industrial automation system.

Demonstrating a Security Solution for Industrial Automation Systems with Intel® Architecture

This demonstration is a product separation industrial machine that sorts a product by its color using vision inspection and control system. It consists of two virtual machines (VM1 and VM2) running on a single computer powered by the 4th generation Intel® Core™ vPro™ processor. The system is set up using open source components that support Intel® TXT and Intel® VT.

Both virtual machines are connected on the same network. VM1 performs the function of a machine vision system that detects the color of the product via a machine vision camera. VM1 then communicates with VM2, which controls an actuator, a conveyer belt, and a warning system. The actuator separates the product into the respective bins for each color based on the information from VM1.

Security Demonstration

In this demonstration, a USB flash drive infected with a rootkit virus is plugged into the computer. The runtime security layer detects the intrusion and prevents the rootkit virus from running automatically. When the computer is restarted, Intel® TXT determines the integrity of the operating system has been compromised and prevents the operating system from loading. This effectively stops the rootkit virus from affecting other parts of the product separation industrial machine.

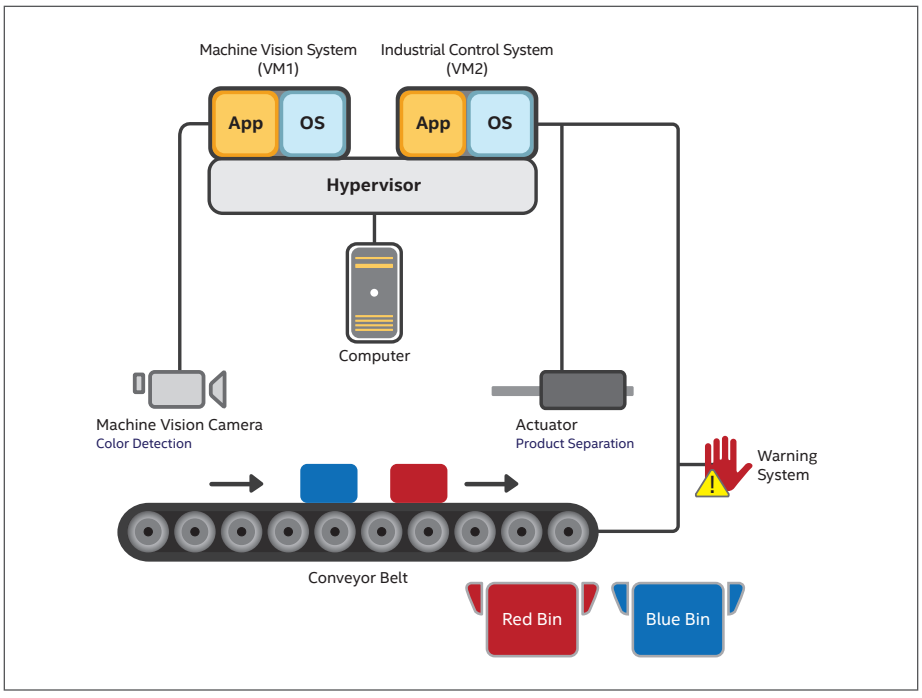
Setting Up the System Using Open Source Components

The computing platform used in the demonstration uses the Hypervisor* from Xen Project, which hosts two instances of virtual machines as the guest operating system. The software required to run the vision inspection is installed into VM1 (machine vision system) and the software to control the conveyer belt is installed into VM2 (industrial control system).

To enable Intel® TXT on both virtual machines to perform a measured and verifed launch of the Hypervisor, an open source pre-kernel module called Trusted Boot* (tboot) is installed. Using Intel® VT, platform resources are securely assigned to each virtual machine, ensuring the trustworthiness of the launch environment.

The following is a general procedure to set up the open source components of the product separation industrial machine that demonstrates the capabilities of Intel® TXT and Intel® VT.

1. Set up the computer BIOS as follows[3]:
   - In Processor configuration, enable Intel® VT and Intel® TXT.
   - In Security, enable TPM.
   - Enable and set up an adminstrator password.
   - Save the settings, and restart the computer.
2. Install Ubuntu* 12.04LTS on the computer that will host the



Demonstration system. This setup comprises a computer based on Intel® Architecture with Intel® vPro™ technology and open source components to protect industrial operations from cyber threats. The computer runs two virtual machines that control the machine vision camera and the actuator of the product separation industrial machine.

operating system for the virtual machines.

3. Install the Hypervisor from Xen Project on the host operating system.
4. Create two virtual machines: VM1 and VM2.
5. Enable PCI passthrough, assigning each VM a dedicated USB controller based on either xHCI or EHCI. Each USB controller controls four USB ports.
6. Enable GFx passthrough, assigning the graphic controller to VM2.
7. In each virtual machine, install the software required to operate the vision inspection and to control the conveyer belt.
8. Set up tboot on the computer. Perform a provisioning process that uses cryptographic hash to measure the untampered hypervisor and the BIOS. When the hypervisor starts, tboot compares the runtime hash with the measured values stored in the Platform Configuration Registers (PCRs) of the TPM.

   Two kinds of measurements are performed:

   - **dynamic measurement:** measures the operating system
   - **static measurement:** measures the core root of trust measurement (CRTM), BIOS, and platform configuration.

9. Restart the computer. Verify that the PCRs are extending and the status of the Intel® TXT measured launch is true. An example is shown below:

   a. Restart the computer.
   ```
   $ reboot
   ```

   b. Select the new menu item created during the tboot installation from the grub menu.

   c. The command `txt-stat` displays information about the status of Intel® TXT (the PCR status) and the tboot log. Run `txt-stat` with the following commands:
   ```
   $tcsd
   $txt-stat
   ```
   An output as shown below indicates the computer performed a measured launch successfully:
   ```
   TXT measured launch: TRUE
   secrets flag set: TRUE
   ```

Conclusion

Security in industrial automation systems is becoming critical as the Internet of Things concept becomes increasingly popular. More components and systems in the manufacturing environment are connected to the Internet, exposing them to external threats of cyber attacks. The challenge is to address the security concerns through a multilayered approach.

Supported by the 4th generation Intel® Core™ vPro™ processor, Intel® TXT and Intel® VT provide hardware-based security and virtualization features that complement existing security measures. These features allow the effective use of computing resources and offer hardware-based security technology to thwart cyber attacks and malicious code. By designing security into its processors, Intel ensures security is inherent in deployed systems based on Intel® Architecture with Intel® vPro™ technology.

For more information on Intel® Trusted Execution Technology and Intel® Virtualization Technology, visit **https://www-ssl.intel.com/content/www/us/en/intelligent-systems/intel-technology/hardware-based-technologies.html**

[1] Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit www.intel.com/technology/vpro.

[2] Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[3] These are generic steps. Refer to the computer's accompanying documentation for the specific information on configuring the computer BIOS.