The Root of Trust: A Foundation for Trusted Computing

Read About

Cybersecurity

TrustedCOTS (TCOTS)

Intel's Trusted Execution Technology (TXT)

Boot Guard

Introduction

Ensuring that an embedded system is trustworthy begins with the first instruction on trusted hardware. An effective trusted computing strategy for COTS solutions can include anti-tamper protection that guards against physical hardware intrusion, encryption techniques for critical data at rest, and effective cyberattack protections that ensure that a corrupted BIOS will cause not harm. The first step to ensure that the BIOS is not corrupted is to establish the hardware "Root of Trust."

Air Force weapon systems today are heavily reliant on complex software and high interconnectivity to perform their missions, making it critical to ensure that their software is trusted and secure.

A foundational concept in cybersecurity, the Root of Trust establishes trusted functions, based on hardware validation of the boot process, to ensure that the system's OS is being started up with uncorrupted code. These functions are located in hardware so they can't be changed.

Protecting embedded systems against cyberattacks must start with the very first instruction that a processor executes. For Intel®-based embedded hardware, two important weapons in the system designer's trusted computing arsenal are Intel's Trusted Execution Technology (TXT) and Boot Guard.

Info

curtisswrightds.com

Email

ds@curtisswright.com

Trusted Execution Technology

TXT provides hardware-based security technologies, built into Intel's silicon and a device called the Trusted Platform Module (TPM). These technologies harden the platform against attacks to the Hypervisor, Operating System or BIOS, as well as malicious root kit installations and other software-based attacks. With TXT, after the code begins executing, the system inspects and "measures" the executed code, comparing it to validate that all is correct.

TXT creates a cryptographic hash (a "measurement" in Intel terminology) of critical BIOS components and compares them to a known good measurement. TXT provides hardware-based enforcement mechanisms to block the launch of code that does not match approved code. This trust can then be extended all the way through the boot loader and into the operating system. Any error in the code will be detected and addressed according to the Launch Control Policy (LCP) established by the user. Because, TXT provides the system integrator with a launch control policy, a notification of corrupted code can have different consequences. After being informed that the system has been modified and is no longer trusted, the user can choose to continue to run or to shutdown. If the system integrator has established an "open" launch policy, the decision to continue to run it is made with full knowledge that the system is no longer trusted.

Boot Guard

Boot Guard works in a complementary fashion to TXT. It is a hardware trust system that inspects an Initial Boot Block to prevent malware and unauthorized software from making any changes Boot Guard runs prior to the BIOS and ensures that the BIOS is trusted before allowing a boot to occur. Intel describes Boot Guard as "hardware-based boot integrity protection that prevents unauthorized software and malware takeover of boot blocks critical to a system's function."

Both TXT and Boot Guard are valuable tools for establishing Root of Trust in Intel-based embedded systems. They are important elements of a comprehensive trusted computing solution. Customers of embedded COTS hardware and system should seek vendors who are informed and knowledgeable about the latest options for protecting their hardware and data from malicious attack or intrusion.

Curtiss-Wright TrustedCOTS

Under its TrustedCOTS (TCOTS) initiative, Curtiss-Wright has instrumented and tested TXT on a select range of Intel processor-based single board computers (SBC) and digital signal processors (DSP).

Intel's 7th Generation Core processor used on select Curtiss-Wright rugged SBCs supports both TXT and Boot Guard.

Curtiss-Wright has developed standard products that include designed-in security features. These products enable system integrators to quickly and economically implement their protection plans for critical technology and data. Curtiss-Wright TCOTS products enable system development to commence with standard COTS hardware and software, and then move to a secure 100% software and performance compatible version of the product when the system integrator is ready to implement their program protection requirements.

To protect Critical Program Information (CPI), Curtiss-Wright builds capabilities into TCOTS hardware from the beginning, using open architecture hardware and software components, with non-proprietary libraries and interfaces.

TXT and Boot Guard Support

Curtiss-Wright is supporting TXT and Boot Guard on a select range of Intel processor-based single board computers (SBC) and digital signal processors (DSP). Contact the factory for more information.

Authors

Steve Edwards, B.S.E.E.
Director, Secure Embedded Solutions
Curtiss-Wright Defense Solutions

Learn More

White Paper:

TrustedCOTS: Leading the Way to Secure Systems

COTS Encyption for Data-at-Rest

Technology:

+ Secured Embedded Solutions
+ Data-At-Rest Encryption