# Trusted boot in COTS computing

MICHAEL SLONOSKY, CURTISS-WRIGHT DEFENSE SOLUTIONS

Military and aerospace system architects and integrators are faced with new challenges as customers implement increasing requirements for safety- and security-critical applications. Military and aerospace embedded computing applications now need to provide both high-assurance computing focused on ensuring overall mission safety along with high availability to safeguard the integrity, confidentiality, and security of the data within and between systems. Moreover, with increased interest in foreign military sales, it is becoming more important to protect critical IP from compromise or alteration.

Another factor driving the need for security assurance is the growth of embedded network-centric computing and the use of open source software in these interconnected systems. Open source software is increasingly treated like a module that can simply be downloaded and plugged into an OEM'sown software. The downside of this approach is that the use of open source code of unknown origin can pose security risks, especially if it has not been analyzed for "back doors."

One approach to mitigating these risks is to implement secure booting so that the system will boot and execute only authentic code. Secure booting prevents the CPU from running untrusted code instead of authentic, OEM-signed code. To achieve this goal, secure booting detects and rejects modified security configuration values and device secrets.

Some examples of high-performance processors that provide secure boot capabilities for military-focused commercial off-the-shelf (COTS) embedded systems include Freescale's QorIQ processors, including the P3041, P4080, P5020, T2080, and T4xxx. Freescale has had years of experience supporting the commercial and automotive computing markets; now the company has integrated trust architecture features into its QorIQ processors. For applications that do not require secure boot, the processors come with secure boot and other trust architecture features disabled by default. When secure boot is enabled, instructions are executed from the internal boot ROM to enable the processor to determine if the image to be loaded into ROM is safe to execute. In the secure state, the image cannot be changed maliciously and the processor can be placed into a state where unauthorized debug or JTAG access is prevented to block snooping or changes to the image to be loaded. Secure boot also prevents the extraction of sensitive values from the CPU by any means short of deprocessing. Once the CPU is in the secure state, a device-specific, one-time-programmable master key (OTPMK) can be used to encrypt and decrypt data.

The starting point for a trusted or secure boot is the creation (by the developer) of a bug-free and malware-free code base. Once the developer "trusts" the code, the developer digitally signs the code so that accidental or deliberate modifications to the code base will be detected during the secure boot cycle. To place a digital signature, an OEM first generates an RSA public and private key pair. It is the responsibility of the OEM to tightly control access to the RSA private signature key. If this key is ever exposed, attackers will be able to generate alternate images that will pass the secure-boot process. If this key is ever lost, the OEM will be unable to update the image.

The application is signed using an RSA private signature key. The digital signature and a hash of the public key is appended to the image and written to flash (or other system nonvolatile memory). When the processor boots, the signature is checked using the RSA public key; the CPU uses the hashed RSA public key to check the signed image and compares the signatures. If the values match, the image is considered authentic and is allowed to boot. QorIQ processors also enable portions of the image to be encrypted to prevent attackers from stealing the image from flash memory.

An example of a COTS single-board computer that supports secure boot is Curtiss-Wright's dual-node VPX6-195 6U OpenVPX board. This single-board computer (SBC) provides antitamper and information security levels by leveraging Freescale's "Trusted Boot" technologies and capabilities. The board features two fully independent processor nodes, each of which has a Freescale quad-core T2080 processor that is provided with its own power, I/O, FPGA, and XMC expansion site.

Figure 1: The dual-node VPX6-195 OpenVPX board leverages Freescale's Trusted Boot capabilities.

(Click graphic to zoom)

Michael Slonosky

Product Marketing Manager for Power Architecture Single Board Computers, C4 Solutions Group Curtiss-Wright Defense Solutions www.cwcdefense.com

THIS ARTICLE WAS PUBLISHED ON OCTOBER 2 nd, 2015.