Becoming a Part of the Transparent Supply Chain

UNICOM Engineering, Inc.
A Division of UNICOM Global

with UNICOM Engineering and Intel

WHY HARDWARE, NOT SOFTWARE, COULD BE THE NEXT BATTLEGROUND FOR NETWORK SECURITY

Counterfeit or compromised hardware has become a critical source of vulnerability for enterprise network systems. Illegitimate hardware components could be potentially harboring malware on them, not to mention that counterfeits cannot deliver the expected levels of performance.

Intel's Transparent Supply Chain initiative is made of six main elements:

- "As-Built" Reports
- Sourcing Data
- Firmware verification
- Trusted Platform Modules (TPM)
- Statement of Conformance (SoC)
- Platform Certificates

Bringing Products, Applications and Ideas to Market Using the Transparent Supply Chain:

Transparent Supply Chain creates opportunities for system integrators, but they must be able to handle the additional administrative burden of verifying each component certificate while ensuring that they do not introduce other compromises during their own hardware build outs.

HARDWARE AS THE NEXT SECURITY BATTLEGROUND

Enterprises who have taken rigorous measures to patch up network and software vulnerabilities still face an insidious and more covert foe in the form of hardware vulnerabilities.

A late 2000's survey revealed 16% of companies purchased counterfeit hardware equipment between 2006 and 2008.

The problem has only increased in recent years, causing Congress and President Obama to sign into law more robust requirements for all Cost Accounting Standards (CAS) purchases by U.S. contractors. As part of due diligence, these purchasers must actively "detect and avoid counterfeit electronic parts" or face potential liability for negative consequences.

BRINGING MUCH-NEEDED TRANSPARENCY TO THE SUPPLY CHAIN, COURTESY OF INTEL

Industry-Leading Oversight Through Transparent Supply Chain

Intel gold standard solution

PLATFORM CERTIFICATE
Intel decided to package all of the relevant documentation along with a confirmed firmware image checksum into a Platform Certificate. This Platform Certificate and its respective assigned public and private keys are needed to complete a three-step verification process that takes place in a Trusted Platform Module (TPM) physically housed on the hardware component.

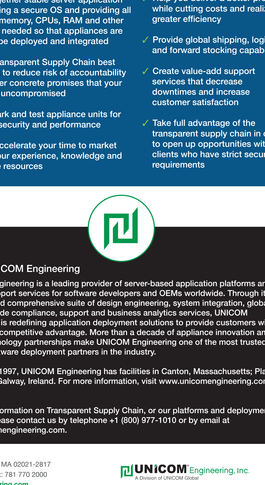
AS-BUILT REPORT
An As-Built report itemizes sourcing, batch numbers and serial numbers for every individual board part during assembly. Without documenting this data during assembly, tracing discrete components becomes much more difficult. As-Built reports cover active components like transistors and ICs, passive components like capacitors and even the PCB itself. As-Built reports are accessible using each individual board's serial number.

FIRMWARE VERIFICATION
Upon final assembly of the board, the Firmware image is verified. Functional test software confirms the programmable device checksums and confirms a match with the board's current firmware revision. This checksum represents a total of all the firmware, creating a unique value that can only be attributed to the current, correct software image.

STATEMENT OF CONFORMANCE
As-Built reports, sourcing documentation and firmware verification test results are all declared in a "Statement of Conformance" pdf given to the end user and signed with a private encryption key provided from Intel's secure database. A Platform Certificate containing similar information and encrypted signatures is also provided for boards using TPM authentication.

How the TPM Protects Appliances Against Hardware Compromises

Before system boot, and before any sensitive information is potentially exposed, this TPM performs three tasks:



CHALLENGES OF GETTING APPLICATIONS TO MARKET USING TRANSPARENT SUPPLY CHAIN

Intel provides digitally-signed Statements of Conformance and Platform Certificates to declare in good faith that any purchased server boards are legitimate and untampered with. Hardware purchasers must then perform due-diligence authentication to confirm that the relevant key pairs are all authentic and working properly.

On top of auditing sourcing documents and performing digital signature authentications, ISVs face countless other hurdles that can balloon costs on their way to market:

1. Creating hardware buildouts
2. Obtaining performance benchmarks and testing units for consistent performance
3. Reliably integrating stable server applications on client environments
4. Implementing branding
5. Determining a lifecycle management strategy or a long-term customer support model
6. Lack of scalable shipping or logistics capabilities

THE SOLUTION: PARTNER WITH TRUSTED INTEGRATORS LIKE UNICOM ENGINEERING

UNICOM Engineering is a value added integrator and deployment partner specializing in streamlining the process of getting ISVs solutions to market while clearing the hurdles that impede success. We function as an extension of your team, providing a comprehensive set of services to design, engineer, ship and support your solutions around the globe.

Through our appliance manufacturing services, UNICOM Engineering can:

- ✓ Piece together stable server application builds using a secure OS and providing all onboard memory, CPUs, RAM and other elements needed so that appliances are ready to be deployed and integrated
- ✓ Follow Transparent Supply Chain best practices to reduce risk of accountability and deliver concrete promises that your parts are uncompromised
- ✓ Benchmark and test appliance units for stability, security and performance
- ✓ Greatly accelerate your time to market through our experience, knowledge and extensive resources
- ✓ Help you deliver a better product while cutting costs and realizing greater efficiency
- ✓ Provide global shipping, logistics and forward stocking capabilities
- ✓ Create value-add support services that decrease downtimes and increase customer satisfaction
- ✓ Take full advantage of the transparent supply chain in order to open up opportunities with clients who have strict security requirements

About UNICOM Engineering

UNICOM Engineering is a leading provider of server-based application platforms and lifecycle support services for software developers and OEMs worldwide. Through its expertise and comprehensive suite of design engineering, system integration, global logistics, trade compliance, support and business analytics services, UNICOM Engineering is redefining application deployment solutions to provide customers with a sustainable competitive advantage. More than a decade of appliance innovation and strong technology partnerships make UNICOM Engineering one of the most trusted, capable software deployment partners in the industry.

Founded in 1997, UNICOM Engineering has facilities in Canton, Massachusetts; Plano, Texas; and Galway, Ireland. For more information, visit www.unicomengineering.com.

Contact Us

For more information on Transparent Supply Chain, or our platforms and deployment services, please contact us by telephone +1 (800) 977-1010 or by email at info@unicomengineering.com.

25 Dan Road, Canton, MA 02021-2817
tel: 781 332 1000 n fax: 781 770 2000
www.unicomengineering.com

UNICOM Engineering, Inc.
A Division of UNICOM Global

intel IoT Solutions Alliance