NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

VALIDATING THE INTEGRITY OF COMPUTING DEVICES

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is developing this publication to demonstrate how organizations can verify that the internal components of computing devices they acquire are genuine and have not been unexpectedly altered during the manufacturing or distribution processes.

BACKGROUND

Product integrity and the ability to distinguish trustworthy products is essential to the foundation of Cyber Supply Chain Risk Management (C-SCRM). By incorporating hardware roots of trust into acquisition and life cycle management processes, organizations can more easily detect supply chain attacks and advanced persistent threats. When these foundational components are leveraged as a computing device traverses the supply chain, trust can be maintained throughout the product's operational life cycle.

CHALLENGES

Modern supply chains are highly complex, introducing the risk of computing device tampering at numerous points. For many of these organizational supply chains, detecting tampering or misconfiguration is one of the most difficult challenges to effectively managing and solving cyber supply chain risks. Assuming that all acquired computing devices are genuine and unmodified increases the risk of a compromise affecting products in an organization's supply chain, which in turn increases risks to customers and end users.

GOAL

This project will demonstrate how organizations can reduce the risk of a compromise to products within their supply chain by producing example implementations of technical mechanisms that can be employed to verify their computing devices are genuine and have not been tampered with. This, in turn, can help to reduce the supply chain risks to customers and end users.

BENEFITS

By implementing the example solution of this project, organizations can:

- verify internal components of their purchased computing devices at subsequent stages in the system life cycle in the operational environment
- implement automated internal processes to analyze, mitigate, and manage supply chain compromises
- protect the confidentiality and integrity of their sensitive data by decreasing the risk of an attack during specific stages of the computing device's supply chain
- limit the cost for recovery from a supply chain attack

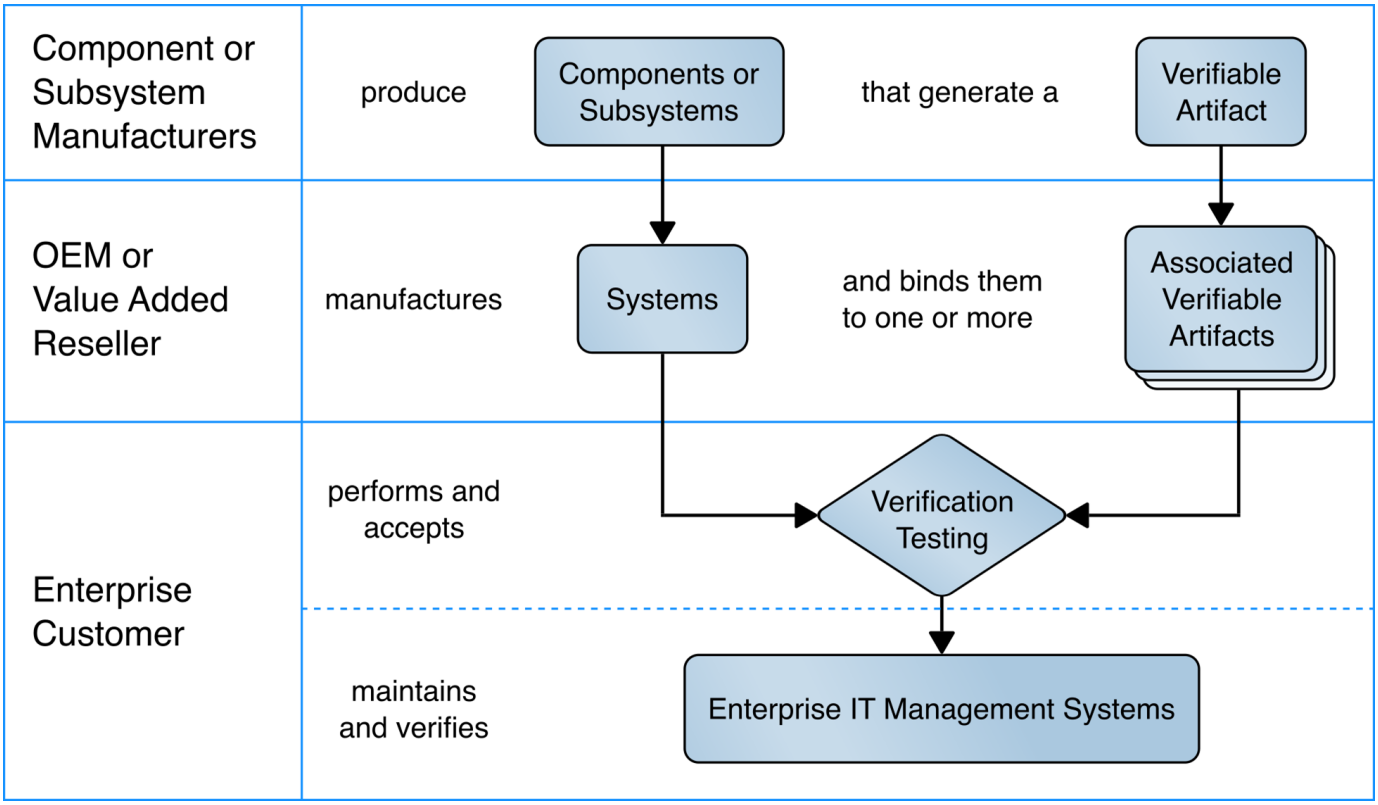
DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/supply-chain-assurance

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email supplychain-nccoe@nist.gov.

DEMONSTRATION COMPONENT ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

Technology Partner/Collaborator	Build Involvement
Dell Technologies	PowerEdge R650, Secured Component Verification tool; Precision 3530, CSG Secured Component Verification tool
Eclypsium	Eclypsium Analytics Service, Eclypsium Device Scanner
HP, Inc.	(2) Elitebook 840 G7, HP Sure Start, HP Sure Recover, Sure Admin, HP Client Management Script Library (CMSL), HP Tamperlock
Hewlett Packard Enterprise	Proliant DL 360 Gen 10, Platform Certificate Verification Tool (PCVT)
IBM	QRadar SIEM
Intel	HP Inc. Elitebook 360 830 G5, Lenovo ThinkPad T480, Transparent Supply Chain Tools, Key Generation Facility, Cloud Based Storage, TSCVerify and AutoVerify software tools
National Security Agency (NSA)	Host Integrity at Runtime and Start-Up (HIRS), Subject Matter Expertise
Archer	Archer Suite 6.9
Seagate Government Solutions	(3) 18 TB Exos X18 hard drives, 2U12 Enclosure, Firmware Attestation API, Secure Device Authentication API

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

May 2022