NIST SPECIAL PUBLICATION 1800-34A

Validating the Integrity of Computing Devices

Volume A:
Executive Summary

Tyler Diamond
Nakia Grayson
William T. Polk
Andrew Regenscheid
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

March 2021

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

Executive Summary

WHY WE WROTE THIS GUIDE

Organizations are increasingly at risk of cyber supply chain compromise, whether intentional or unintentional. Cyber supply chain risks include counterfeiting, unauthorized production, tampering, theft, and insertion of unexpected software and hardware. Managing these risks requires ensuring the integrity of the cyber supply chain and its products and services. This project will demonstrate how organizations can verify that the internal components of the computing devices they acquire are genuine and have not been unexpectedly altered during manufacturing or distribution processes.

CHALLENGE

Technologies today rely on complex, globally distributed and interconnected supply chain ecosystems to provide highly refined, cost-effective, and reusable solutions. Most organizations' security processes consider only the visible state of computing devices. The provenance and integrity of a delivered device and its components are typically accepted without validating through technology that there were no unexpected modifications. Provenance is the comprehensive history of a device throughout the entire life cycle from creation to ownership, including changes made within the device or its components. 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.

Organizations currently lack the ability to readily distinguish trustworthy products from others. Having this ability is a critical foundation of cyber supply chain risk management (C-SCRM). C-SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of supply chains. C-SCRM presents challenges to many industries and sectors, requiring a coordinated set of technical and procedural controls to mitigate cyber supply chain risks throughout manufacturing, acquisition, provisioning, and operations.

This practice guide can help your organization:

- Avoid using compromised technology components in your products
- Enable your customers to readily verify that your products are genuine and trustworthy
- Prevent compromises of your own information and systems caused by acquiring and using compromised technology products

SOLUTION

To address these challenges, the NCCoE is collaborating with technology vendors to develop an example solution. This project will demonstrate how organizations can verify that the internal components of the computing devices they acquire are genuine and have not been tampered with. This solution relies on

device vendors storing information within each device, and organizations using a combination of commercial off-the-shelf and open-source tools that work together to validate the stored information. By doing this, organizations can reduce the risk of compromise to products within their supply chains.

In this approach, device vendors create an artifact within each device that securely binds the device's attributes to the device's identity. The customer who acquires the device can validate the artifact's source and authenticity, then check the attributes stored in the artifact against the device's actual attributes to ensure they match. A similar process can be used to verify the integrity of computing devices while they are in use.

Authoritative information regarding the provenance and integrity of the components provides a strong basis for trust in a computing device. Hardware roots of trust are the foundation upon which the computing system's trust model is built, forming the basis in hardware for providing one or more security-specific functions for the system. Incorporating hardware roots of trust into acquisition and lifecycle management processes enables organizations to achieve better visibility into supply chain attacks and to detect advanced persistent threats and other advanced attacks. By leveraging hardware roots of trust as a computing device traverses the supply chain, we can maintain trust in the computing device throughout its operational lifecycle.

This project will address several processes, including:

- how to create verifiable descriptions of components and platforms, which may be done by original equipment manufacturers (OEMs), platform integrators, and even information technology (IT) departments;
- how to verify devices and components within the single transaction between an OEM and a customer; and
- how to verify devices and components at subsequent stages in the system lifecycle in the operational environment. This project will also demonstrate how to inspect the verification processes themselves.

The following is a list of the project's collaborators.

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-34a: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-34b: Approach, Architecture, and Security Characteristics* once it is made available. It will describe what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-34c: How-To Guides* once it is available. It will provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance. Help the NCCoE make this guide better by sharing your thoughts with us. There will be at least one additional comment period for this volume, and the other volumes of this guide will be released for review and comment on individual schedules so that each volume is available as soon as possible. Volumes B and C are under development and they will be published when they are ready.

Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments, join the community of interest, or learn more about the project and example implementation, contact the NCCoE at supplychain-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.