BUILDING BLOCK

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SOFTWARE ASSET MANAGEMENT

Continuous Monitoring

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of software asset management through collaboration with members of the IT community, including vendors of cybersecurity solutions. The result will become an NCCoE "building block": an approach that can be incorporated into multiple use cases. The solution proposed by this effort will not be the only one available in the fast-paced cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at conmon-nccoe@nist.gov.

SECURITY CHALLENGE

Businesses can't protect what they don't know they have. A successful software asset management (SAM) system can help organizations inventory and assess the state of installed software across their IT systems, providing accurate, timely information about the current state of the software installed, authorized and used on the computing devices that access organizational resources and support critical business functions. Businesses that automate collection and secure exchange of software inventory data can automate common business processes to authorize the execution of software, and better understand which patches and software updates are needed to minimize software vulnerabilities, and what software configurations need to be applied to ensure compliance with organizational configuration policies.

The software lifecycle has several stages from release, to installation, to maintenance with patches and updates, to uninstallation when the product is no longer of use. Managing these milestones requires a variety of business processes: Licenses are tracked and purchased as needed as part of a license management process; software media is acquired as part of a supply chain; software is updated to take advantage of new features as part of a change management process; and patches are applied to fix security and functional flaws as part of vulnerability and patch management processes. In many organizations, SAM processes are either manual or are supported by a collection of proprietary solutions. Proprietary solutions often lack integration with other operational and security systems, are aligned with specific product families, and provide different informational views into the software they manage.

OUR APPROACH

This building block proposes a standardized approach to software asset management so that an organization has an integrated view of software throughout its lifecycle. The building block will support:

- authorization and verification of software installation media that verifies that the media is from a trusted software publisher and that the installation media has not been tampered with
- software execution whitelisting that verifies that the software is authorized to run and has not been tampered with
- publication of installed software inventory to an organization-wide database
- software inventory-based network access control that dictates a device's level of access to a network based on what software is or is not present on the device and whether its patches are up-to-date

The data format at the core of this solution is the software identification (SWID) tag, an XML-based data format containing a collection of information that identifies a specific unit

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

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

of software and provides other data elements that enable categorization, identification and hashing of software components, references to related software and dependencies, and other data points. SWID tags can be associated with software installation media, installed software and software updates (e.g., service packs, patches, hot fixes).

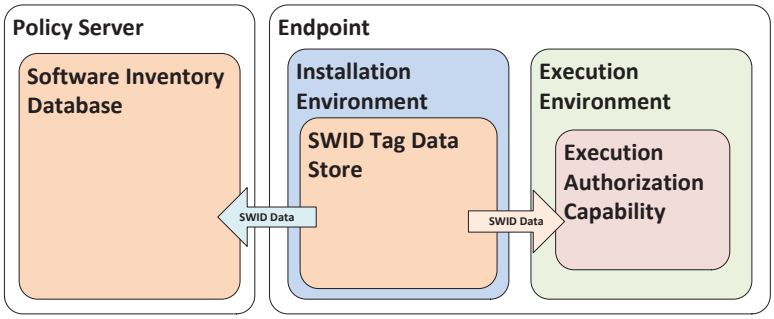
Secure transport protocols are required to enable SWID tag data to be exchanged. The Trusted Network Connect (TNC) specifications provide the standards-based mechanisms to support the secure exchange of SWID tag information. The TNC standards enable accurate software inventory information to be made available to the enterprise. Using the TNC protocols, collected SWID tag data can be published to a data store managed by a policy server. This persisted information can be used to support configuration, vulnerability management, attack detection, network access control decision making, and other security automation tasks.

The building block's SAM capabilities, based on SWID tags and TNC transport protocols, will:

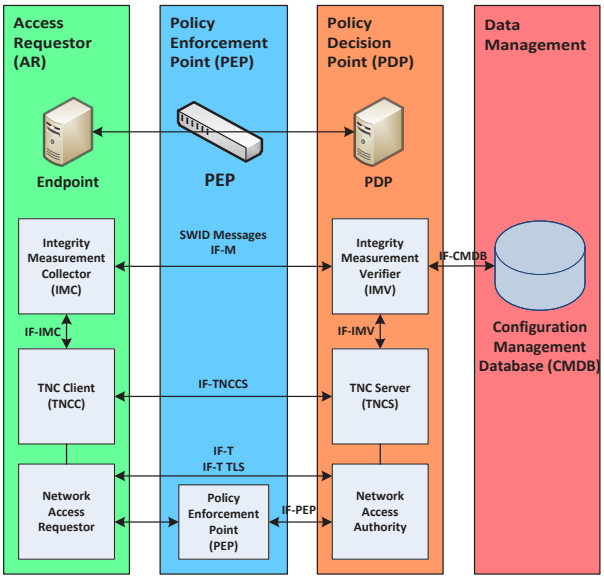
- allow installation media to be verified as authentic
- enable software execution to be limited to authorized software based on organizational policies
- demonstrate a standardized approach for securely collecting and exchanging software inventory data from networked endpoint devices, including those accessing a network remotely
- enable use of authoritative, vendor-provided SWID tag information to drive business processes
- make exchanged software inventory data available to operational and security systems where it can be evaluated against organizational policies supporting human-assisted and automated, risk-based decision making

The solution must conform to the Trusted Computing Group (TCG) Trusted Network Connect (TNC) Endpoint Compliance Profile (ECP). Data collection of SWID tag-based software inventories must occur based on software installation change events.

HIGH-LEVEL ARCHITECTURE



- The endpoint represents the computing device for which the software inventory is monitored.
- The policy server monitors and enforces software-related policies, and is the point of publication for software inventory data generated at the computing device.
- Collected SWID tag data is published in the data store.
- The execution environment restricts execution of software that was not installed or modified using authorized mechanisms.
- The execution authorization capability verifies the integrity of software prior to execution using cryptographic hashes associated with the SWID footprint.
- It is expected that multiple computing devices will interact with a single policy server.
- Organizations may choose to implement multiple policy servers responsible for maintaining software inventory data for a network, office, data center or other organizational scope.
- The data stored on the policy server will support many different analysis processes.



The TNC architecture that is used to transport software inventory data and to support network access control functionality supported by this building block.

LEARN MORE ABOUT THIS PROJECT

http://csrc.nist.gov/nccoe/Building-Blocks/conmon.html

HOW TO PARTICIPATE

Contact conmon-nccoe@nist.gov and watch the Federal Register for a notice inviting participation from the cybersecurity technology community.