InfusionPoints
CyberSecurity Solutions

A report for Hewlett Packard Enterprise

HPE is Elevating Supply Chain Security

Supply Chain Under Attack

Supply chain attacks dominated headlines in 2020 and this has continued into 2021; with events like the Solarwinds attack, reports on the emergence of counterfeit hardware[1], and the critical infrastructure ransomware attack on the Colonial Pipeline. Supply chain attacks have increased 42% in the first quarter of 2021 according to analysis of data from the Identity Theft Resource Center (ITRC)[2] – a trend that appears to be here to stay. More troubling, cyberattacks overall appear to be increasingly targeted, meaning that attackers are no longer relying on easy win targets of opportunity, and are instead going after big payoffs. This is prompting aggressive action by governments as evidenced by the recent US Executive Order on Improving the Nation's Cybersecurity[3] in which Zero Trust architectures are a key focus area to improving and modernizing Government cybersecurity capabilities. In fact, the Zero Trust concept is mentioned 11 times, and is defined in Section 10 (k) of the Executive Order as:

> *"The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources... ... The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly ... looks for anomalous or malicious activity." ~Executive Order on Improving the Nation's Cybersecurity, May 12, 2021*

These threats to the supply chain mean that vendors must build the technology and feature sets that enable Zero Trust architectures and mechanisms that continuously validate the secure, trustworthy state of their products throughout their lifecycle. For hardware suppliers, this means that features must be included to validate the hardware and firmware of the shipped products continuously.

HPE started building the foundation of Zero Trust capabilities with the release of the HPE-exclusive Silicon Root of Trust in 2017 with HPE ProLiant Gen10 servers which we thoroughly tested at the time. We found that their Silicon Root of Trust provides validation and recovery capabilities for the server UEFI and HPE Integrated Lights Out (iLO) firmware and extends to provide this validation to component firmware as well. With HPE ProLiant Gen10 Plus servers, HPE continues to add Zero Trust enabling features into their inter-generation products.

Figure 1 – HPE ProLiant DL380 Gen10 Plus.

HPE recently invited us to take a look at their latest innovations including new server product cryptographic identities and platform certificates.

HPE Platform Certificates

HPE has announced the introduction of the HPE Server Platform Certificate, along with HPE Server Cryptographic Identities on HPE ProLiant Gen10 Plus servers. This is in addition to a Trusted Platform Module (TPM) being included as standard with all HPE ProLiant Gen10 Plus servers. As a supporter of the Trusted Computing Group (TCG), HPE has worked to ensure an open standards based TCG compliant implementation of platform certificates

[1] https://labs.f-secure.com/publications/the-fake-cisco/
[2] https://www.cips.org/supply%2dmanagement/news/2021/april/troubling-rise-in-supply-chain-cyber-attacks/
[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

providing the means for customers to validate the state of their servers at any point in their lifecycle.

Adhering to the Trusted Computing Group (TCG) industry standards, HPE helps customers to reduce their total cost of ownership while supporting many compliance needs. The Platform Certificate is based on the hardware manifest at the birth of the server. The TCG compliant HPE Platform Certificate is generated using a highly protected Certificate Authority and stored in non-volatile memory on the server and is made easily accessible to the customer through HPE iLO. Each system is also validated against the hardware manifest prior to shipping. Within the United States, these systems will be manufactured leveraging the HPE Trusted Supply Chain program which gives customers stronger validations with hardened security features directly enabled within the factory by vetted HPE employees in highly secure facilities on U.S. soil.

Upon arrival at the customer site, using industry standard tools like (HIRS/PACCOR) administrators runs a verification process to provide the ability to validate the integrity of the system throughout the Supply Chain Life Cycle. Leveraging HPE's Silicon Root of Trust, administrators can validate that the integrity of the firmware loaded into the UEFI has not been tampered with and can also verify that the hardware manifest is in a valid state. Administrators can then utilize industry standard tools to ensure no hardware changes have been made.

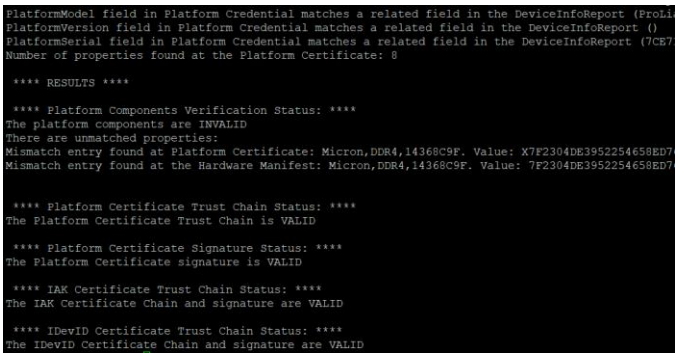

Figure 2 - HPE Platform Certificate Verification Process

As shown in Figure 2, when hardware changes have been made the platform verification will report an INVALID status, providing information about which piece of hardware or component has been modified since the birth of the system within the secure supply chain manufacturing process. This provides the customer with confidence that the system has not been altered or tampered with prior to connecting to the network.

HPE Product Cryptographic Identity

During the process of TCG Compliant Platform certificate creation and generation of the hardware manifest, HPE also provisions device identifiers known as IDevIDs to the server and to iLO. IDevIDs are lifetime credentials that provide identification and authentication of the server and iLO to data and management plane platforms like provisioning systems that are managed by the customer. These may also be used to authenticate the device to HPE's as-a-Service offerings like HPE GreenLake Cloud Services.[4] When combining use of platform certificates and device identities, customers have a way to validate the authentic condition of the server, and securely authenticate that server and iLO to other systems, both of which are key enabling capabilities of Zero Trust architectures.

Learn more about InfusionPoints analysis of HPE's Cryptographic Identities

Industries that require Zero Trust architectures will benefit from this new Platform Verification Process, that ensures that systems have not been altered at any point since leaving the factory and prior to connecting to mission critical networks such as government networks critical infrastructure.

Furthermore, we have found that HPE's additional steps to protect systems during the supply chain process utilizing their Platform Certificate Validation Process, fully covers MITRE ATT&CK TTPs 1200 (Hardware Additions) and 1199.003 (Compromise Hardware Supply Chain).

Conclusion

HPE continues to prove their responsible approach to ensuring the security of their customers infrastructure.

[4] https://psnow.ext.hpe.com/doc/a00114962enw

Staying up to date with leading industry tactics, techniques and current threats allows HPE to continue to adapt and invest in future hardware design and manufacturing technologies. As supply-chain attacks continue and adversaries pivot to new tactics, seeing HPE's approach to staying one step ahead should allow consumers to rest easy knowing HPE has their interest.

About HPE

HPE Increases your business agility by integrating scalable security throughout your organization at every step in your IT journey. HPE's products and services leverage common security building blocks – from silicon to cloud – that continuously protect your infrastructure, workloads, and data, adapting to increasingly complex threats. HPE has the technology and expertise to capitalize on your prior investments and reinforce your existing strategy, transforming security from a barrier to an accelerator of Innovation. Learn more: https://www.hpe.com/security

About InfusionPoints

InfusionPoints is your independent trusted partner dedicated to assisting you in building your secure and compliant business solutions, testing your security controls, and defending your consumer, employee, and supply chain information.

Important Facts about this Paper

PUBLISHER: InfusionPoints, LLC

INQUIRIES: Contact us if you would like to discuss this report, and InfusionPoints will respond promptly.
+1-336-990-0252
info@InfusionPoints.com
https://www.infusionpoints.com

DISCLOSURES: This paper was commissioned by Hewlett Packard Enterprise (HPE). InfusionPoints provides security research, analysis, advising, consulting, and penetration testing to many high-tech companies in this space.

DISCLAIMER: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. InfusionPoints, LLC disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of InfusionPoints, LLC and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

InfusionPoints, LLC provides forecasts, and forward-looking statements, and trends in cybersecurity as directional indicators and not as precise predictions of future events. While our opinions are based on our current judgment based on available information and analysis, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinion as of the date of publication for this document.

Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.