SOLUTION BRIEF

Secure the Network Infrastructure – Secure Cloud Native Network Platforms

Using Intel® Security Libraries for Data Center to build end-to-end platform security with Kubernetes* orchestrated infrastructure

Executive Summary

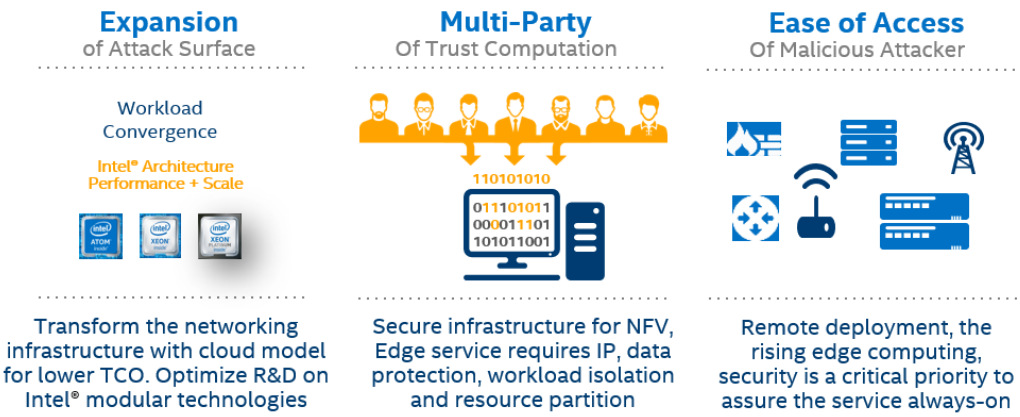
Security for cloud native applications is an increasing challenge for developers. Hardware and software suppliers in the industry are cooperatively developing the cloud architecture to deliver 5G network and edge infrastructure, which makes security an important requirement as workloads and suppliers converge.

This document describes the Hardware Root of Trust, Secure Boot, and Intel® Security Libraries for Data Center (Intel® SecL - DC), which can be used to create an end-to-end open source security solution that is already integrated for Kubernetes clusters, making it a preferred platform security solution for network and edge platforms.

This document is part of the Network Transformation Experience Kit, which is available at https://networkbuilders.intel.com/network-technologies/network-transformation-exp-kits.

Introduction

Common platform and open source ingredients have transformed the networking infrastructure. From a security perspective, this transformation has also increased the risk of security attacks. Workload convergence issues can arise when network and edge services are consolidated on server platforms. Network and edge platforms can be deployed in a more distributed and less secure facility than a data center, which leads to additional security concerns about expanded attack surface, multiple parties to be trusted, and malicious attacker access, as shown below.



Rise of Cloud Native Networking

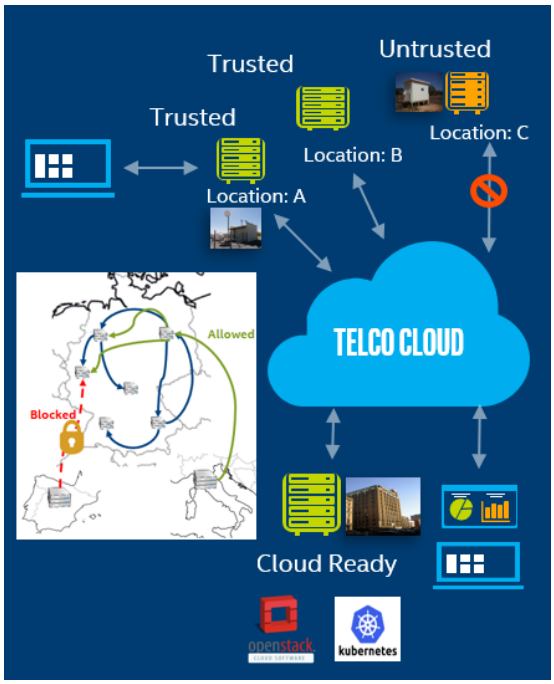
Container-based technologies have advanced cloud computing architecture. Cloud native network functions and Network Functions Virtualization Infrastructure (NFVI) have been adopted for the preliminary 5G network infrastructure as well. Kubernetes has emerged as a preferred choice to orchestrate virtual machine (VM)/container workloads and to manage the pod and server infrastructure. Containers are designed to be lightweight and scalable, which makes security an integral challenge for container-based network and edge platforms.

Security Challenges

The working group National Cybersecurity Center of Excellence (NCCoE) is part of the National Institute of Standards and Technology (NIST). The working group has released a 5G Cybersecurity project paper, which recommends that "The supporting infrastructure will utilize hardware roots of trust for platform measurement and attestation to ensure that certain workloads run on hardware in a good known state and within a well-defined logical boundary."

Cloud native platforms can be deployed in different types of network locations, such as base stations for telco networks and on-site at stadiums or factories. Therefore, the security solution must align with the end-to-end deployment model. In addition, the platform security status must report to Kubernetes-based management software. Specific challenges include the following:

- Platform integrity: At a high-level, the platform consists of hardware, firmware, and software. Any platform tampering, firmware, or OS hacking should be detected and reported. During initial deployment, security hardening is implemented with the best intentions, however, security threats are dynamic and always evolving. The never-ending cycle of cybersecurity attacks expose more system vulnerabilities over time. There were 170 Linux* vulnerabilities reported in 2019 [Source]. If deployed systems are exposed with vulnerabilities discovered later by security researchers, security fixes must be made to secure the platform.
- Central cloud control: The network platform is deployed at geographically dispersed locations, so remote management must include security policy. From a network and edge platform monitoring perspective, platform integrity is an essential service. Integration with Kubernetes is important, as the network administrator can scan/audit the worker node's security status and apply security updates (such as firmware, OS patches, and others) in a timely fashion.
- Location and security policy: From the network function and/or edge service perspective, software placement is owned by the network operator. The operator has the responsibility to ensure the workload is placed onto a platform with the appropriate security control and to prevent important IP (such as an AI model) and data from being exposed on a compromised platform, which could lead to theft of IP or data.



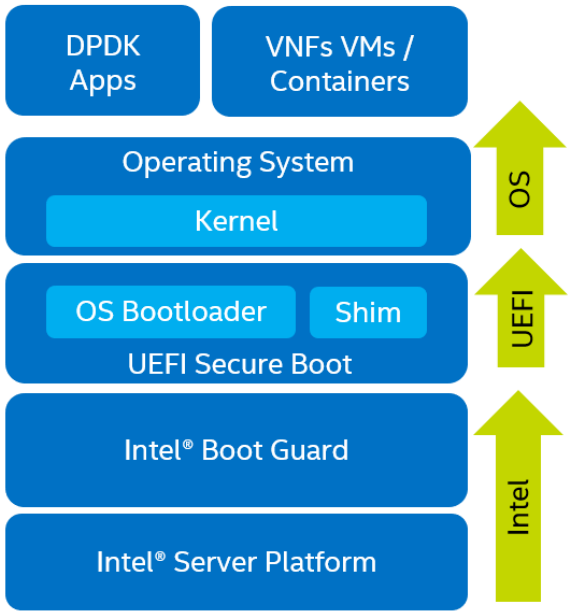
Solution Description

End-to-end platform security is essential for networking. Security can be further broken into areas for "protecting data" and "securing the platform", where the platform includes CPU, memory, networking I/O, and disks for data storage.

Intel recommends using Secure Boot Methodologies at every level in the software stack. When implemented, a Hardware Root of Trust connects the platform hardware, firmware, and software with the trust chain, so that only authorized firmware and software can execute on the CPU. The trust is built from the silicon level, using technologies such as Intel® Boot Guard technology, which is supplied by Intel® Xeon® Scalable processors.

Secure boot is critical, and an additional step is the integration of platform attestation into the cloud software, such as Kubernetes. As discussed earlier, the platform may contain system vulnerabilities that may be exposed after the initial deployment. A platform integrity monitoring service is essential, so that if a vulnerability is discovered by security researchers, then the network operator can take quick action to identify the impacted platforms, apply a security fix, or even bring the platform down.

Kubernetes integrates these types of platform integrity services at the orchestration level of a cloud native networking platform.



Technologies Implemented

Intel® Security Libraries for Data Center (Intel® SecL - DC) is an open source security solution that was released in April 2019. Intel® SecL - DC consists of software components providing end-to-end cloud security solutions with integrated libraries. Users have the flexibility to either develop their customized security solutions with the provided libraries or deploy the software components in their existing infrastructure.

One of the Intel® SecL - DC features is platform integrity attestation. This is achieved by leveraging hardware root of trust to measure the platform boot phase, and write the firmware/Linux kernel signature into the Trusted Platform Module (TPM), a security chip installed at the server platform. Intel® SecL - DC provides an end-to-end platform security service that is already integrated for Kubernetes clusters, making it a preferred platform security solution on Intel network and edge platforms.

Key components of Intel® SecL - DC include the following:

- **Verification service:** Installed in the central control node, it gathers the secure boot signatures and maintains the platform's "trusted" or "untrusted" evaluation results. It maintains the platform trust database with established "known good" values or expected measurements (which are called flavors in Intel® SecL – DC). If a certain firmware or Linux kernel are found to be compromised, the policy here can change the platform trust status.
- **Trust agent:** Installed in every physical node that needs to be monitored by the platform security. It takes the TPM ownership on the platform and reports the platform security status to the remote management module.
- **Integration hub:** Connects with orchestration software such as Kubernetes or OpenStack* and contains an extension to work with K8s. It retrieves the information from the verification service and shares with the orchestration software at a specified interval.

Use Case Examples

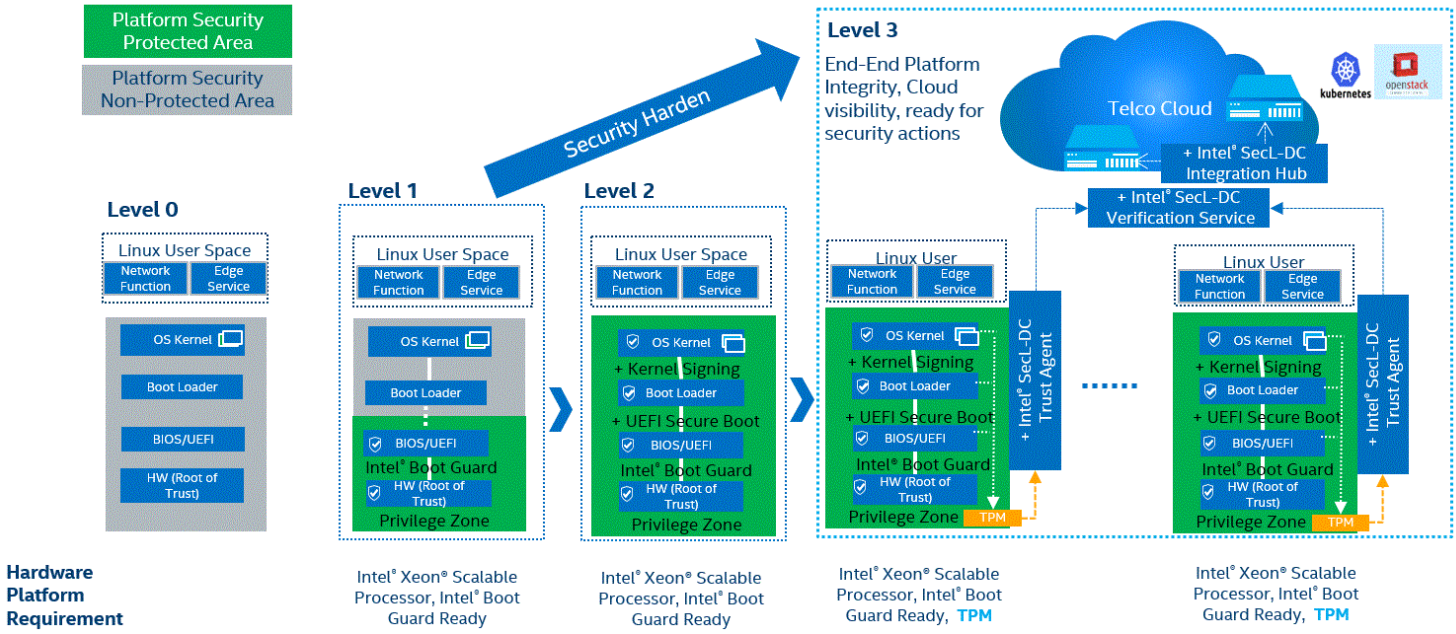
Many platform security technologies are available in the marketplace, which puts a burden on telecom operators who are responsible for defining their optimal security strategy. Implementing a solution requires industry collaboration from both hardware and software manufacturers, because a good security solution must be simple, effective, easy to use, affordable and sustainable. After completing extensive study on security technology ingredients, Intel recommends using different security defensive levels in the marketplace as a framework for driving your security policy, as shown in the following diagram.

- **Level 0:** is the default platform set up without using any known platform security technologies.
- **Level 1:** Choose an Intel® Boot Guard ready server so that hardware root of trust is in place for more firmware protection. This can be achieved using an Intel® Xeon® Scalable Processor-based server platform.
- **Level 2:** Extend the root of trust to secure the complete NFVI stack, using UEFI secure boot to help protect the Linux kernel. Ensure that firmware and kernels are always from trusted suppliers to help secure the network/edge nodes and avoid platform tampering.

- **Level 3:** Verify and monitor platform integrity regularly to help secure the platform at the node level. Cloud centric visibility is an important factor. Incorporate platform attestation with Kubernetes orchestration to help deliver end-to-end platform security, enable more timely security patching, and help reduce platform vulnerability.

Refer to http://software.intel.com/en-us/articles/optimization-notice for more information regarding performance and optimization choices in Intel software products.

Platform Security: Defensive Levels



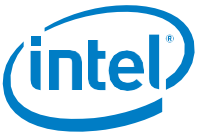
Summary

Building a platform security solution requires a time investment for researching and creating a comprehensive plan. This document recommends choosing a server platform that uses Intel® Xeon® Scalable Processors, enabling hardware root of trust with Intel® Boot Guard technology, and building with secure boot to extend the trust to cover the entire software stack.

Applying Intel® SecL-DC takes it a step further, by integrating platform attestation into the cloud native architecture and using Kubernetes to orchestrate and run the workload on the trusted pod. The solution described in this document is also applicable to bare-metal, VM-based networking architectures with a seamless integration to OpenStack* managed cloud infrastructure.

For detailed instructions on using Intel® SecL-DC with Kubernetes, refer to Secure the Network Infrastructure – Secure Cloud Native Network Platforms User Guide.

REFERENCE	LINK
5G CYBERSECURITY Preparing a Secure Evolution to 5G	https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-draft.pdf
Secure the Network Infrastructure – Secure Boot Methodologies Application Note	https://builders.intel.com/docs/networkbuilders/secure-the-network-infrastructure-secure-boot-methodologies.pdf
Secure the Network Infrastructure – Secure Cloud Native Network Platforms User Guide	https://builders.intel.com/docs/networkbuilders/secure-the-network-infrastructure-secure-cloud-native-network-platforms-user-guide.pdf



0420/DN/PTI/PDF 621827-001US