SOLUTION BRIEF

Security Considerations for Network Functions Virtualization for Communications Service Providers

Table of Contents

Revision 1.0 October 2016

Executive Overview

Intel is accelerating the adoption of Network Functions Virtualization (NFV) with unique capabilities that enable optimal use of data center resources to deliver Communications Service Provider (Comms SP) services based on standard high-volume servers. Virtualization provides capabilities that will reduce costs (Capex, Opex) and enable greater flexibility to create and grow new services by running previously hardware-dependent functions in a virtualized software model. This briefing is focused on identifying the security enhancements and best practices specific to Comms SPs' NFV environments.

This document is aimed at service providers who may be evaluating NFV-related projects with a desire to understand the relevant security considerations, including the Intel® technologies available to harden virtualized environments. This document highlights Intel's technologies and capabilities in the security domain and its security-related efforts to accelerate adoption of NFV and to realize the many business benefits of virtualized applications in production deployments.

State of the Industry

NFV and Software-Defined Networking (SDN) provide the portability, flexibility, and programmability for the rapid deployment of network-based services. NFV and SDN also enable the ability to scale seamlessly the network functions required to deliver the business requirements demanded by increased application usage and extensive connectivity requirements. The use of standard high-volume servers (SHVS) combined with a common and flexible horizontal infrastructure enable network functions to be deployed from the edge of the network to the data center through a virtualized cloud-based infrastructure.

The market opportunity for virtualization and the commitments made across the industry by global Comms SPs to the network transformation is well documented. For example, recent research by the Open Platform for NFV* (OPNFV*) Project found that 94 percent of service providers had an NFV strategy.[1] One proof point is AT&T,[2] which is collaborating closely with Intel and has a stated goal of virtualizing 75 percent of its network by 2020. The business drivers for network transformation, such as reduced cost, increased network flexibility, and shortened time to market for new services, are the primary catalysts for the technology transformation required to enable Comms SPs to launch new and innovative revenue-generating services.[3,4]

However, to achieve the vision and the many benefits of NFV, security remains a top concern and has been a hurdle to the adoption of network transformation. Based on a recent Heavy Reading survey, security is one of the largest concerns impacting the broad adoption of NFV.[5] At the OPNFV Summit in January 2016, security was cited as the top technology concern that OPNFV should investigate.[6]

For example, the attack surface areas and broad exposure to vulnerabilities may be increased in a virtualized environment, compared with a closed physical network function environment. There are many key security considerations required to adequately address the security challenges required to harden the "network" and enable the realization of a Comms SP's horizontal NFVI infrastructure.

Intel's Role in Addressing NFV and SDN Security

SDN and NFV provide the framework and the capabilities to programmatically control and automate the placement of network functions that will improve user experience, provide additional security controls, and enable the scaling of network services based on business drivers or application requirements. The server platform resources that are exposed through the virtual infrastructure management (VIM) and managed through the service orchestration function enable virtual network functions (VNFs) to scale incrementally with consumption. Software-based network controllers interact with the underlying virtual (or physical) routing and switching functions to steer traffic appropriately.

The shared resources of the horizontal infrastructure and multivendor software stack in a virtualized environment open a different set of attack points and security vulnerabilities for Comms SPs. As identified by the European Telecommunications Standards Institute (ETSI)-NFV,[7] the investigation into security for NFV covers several different domains. Intel is addressing these concerns through technology, open source contributions, and industry-standards efforts. Some of the NFV security efforts contributed by Intel include:

- Topology validation and enforcement
- Availability of management support infrastructure
- Secured boot
- Attestation
- Secure crash
- Performance isolation
- User/Tenant authentication, authorization and accounting (AAA)
- Authenticated time service
- Private keys within cloned images
- Back-doors via virtualized test and monitoring functions
- Multi-Administrator isolation
- Security monitoring
- Regulatory (lawful intercept and retained data)
- Privacy

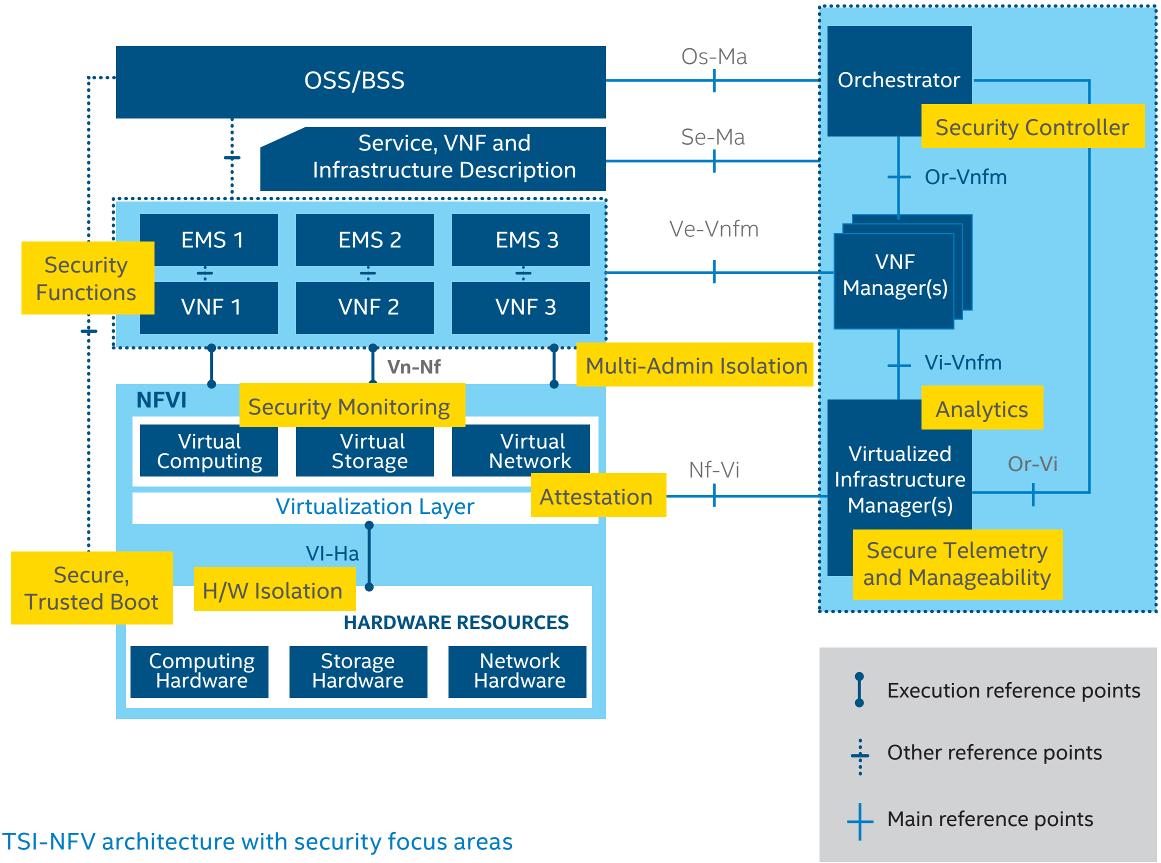


Figure 1. ETSI-NFV architecture with security focus areas

The cost and performance advantages of virtualization also introduce new security challenges that require a new approach to developing the layers of security, attestation, and domain isolation. Figure 1 overlays the traditional ESTI-NFV architecture with identified security-related focus areas. These are the broad areas of focus across industry standards bodies, open source consortia, and within Intel to address security across the NFVI and VNF stacks.

Intel's efforts to drive security innovation across the industry are helping to address the areas highlighted above in order to harden the virtualized environment for Comms SP deployments and proactively tackle potential security concerns. In addition to technology, Intel is working across the ecosystem to develop and align best practices for configuration settings, security workload performance, and access controls that should be followed to insure a secure, highly performing environment with optimal data center resource utilization.

Intel® Technologies and Ecosystem Enablers

To provide a high-level of security within an NFV environment, Comms SPs must deploy sophisticated security measures to protect the platform, optimize the performance for the security function and workloads, and provide application and function isolation. Common hardware security considerations for NFV and SDN are identified in Table 1.

Platform Security and Attestation

Virtualization, using industry-standard servers, provides Comms SPs with the capability to deploy VNFs inside and outside the data center across different geographies. Hardware security assistance and root of trust technologies are necessary components to insure the validity of the platform's software stack. This includes not only the validation of the hardware, but also the BIOS, hypervisor, OS, and software images. This section describes Intel® Trusted Execution Technology (Intel® TXT), Intel® Cloud Integrity Technology (Intel® CIT), Intel® Clear Containers, and Intel® Resource Director Technology (Intel® RDT) as key technologies to enable a trusted environment for SDN and NFV.

Intel® Trusted Execution Technology

Intel TXT provides hardware identification to limit workloads to authorized locations and devices. For virtualized workloads, each platform must have a component that will always behave in the expected manner and contain a minimum set of functions enabling a description of the platform characteristics and its trustworthiness. Intel TXT can serve as a hardware-based root of trust to validate software platforms and workloads at boot.

The system checks launch time configurations against a "known good" sequence to quickly assess whether any attempts to alter or tamper with the launch time environment have been made. Intel TXT verifies system BIOS and firmware and launches the OS.

Security Area	What	Description	Why
Platform Security and Attestation	Intel® Trusted Execution Technology (Intel® TXT)/ Intel® Cloud Integrity Technology	Intel TXT validates the behavior of key components within a server at startup.	Provides the "root of trust": the system checks launch time configurations against a "known good" sequence to quickly assess whether any attempts to alter or tamper with the launch time environment have been made.
Hardening and Acceleration	Instruction sets (e.g. Intel® Advanced Encryption Standard New Instructions)	Core crypto performance enhancements to improve the compute efficiency of cryptographic algorithms.	Enables greater protection for application data, data moving across a network, and stored data.
	Hardware Accelerators (e.g. Intel® QuickAssist Technology)	Scalable hardware accelerators exposed to Intel® architecture as PCIe* devices, providing acceleration.	Resource optimization application and performance optimization for network security, such as IPSec, SSL/TLS, IDS/IPS, firewall.
Multi-Admin Isolation	Intel® Virtualization Technology (Intel® VT), Intel® Software Guard Extensions	Eliminating virtualization performance overhead and improving security with hardware assist to the virtualization software, reducing its size, cost, and complexity.	Provide and improve security in shared resource environment, e.g., utilizing Containers with Intel VT enables secure resource optimization deployment models.

Table 1. Intel® technologies addressing security challenges

Intel TXT works by creating a measured launch environment (MLE) that enables an accurate comparison of all the critical elements of the launch environment against a known good source. Intel TXT creates a cryptographically unique identifier for each approved launch-enabled component, which it holds in the trusted platform module (TPM) to provide hardware-based enforcement mechanisms to block the launch of code that does not match approved code.

This hardware-based solution provides the foundation on which trusted platform solutions, such as Intel CIT, can be built to protect against the software-based attacks that threaten integrity, confidentiality, reliability, and availability of systems.

For environment attestation, Intel TXT enables platform measurement credentials to be provided to local or remote users or systems to complete the trust verification process and support compliance and audit activities. Figure 2 provides a description of how Intel TXT works.

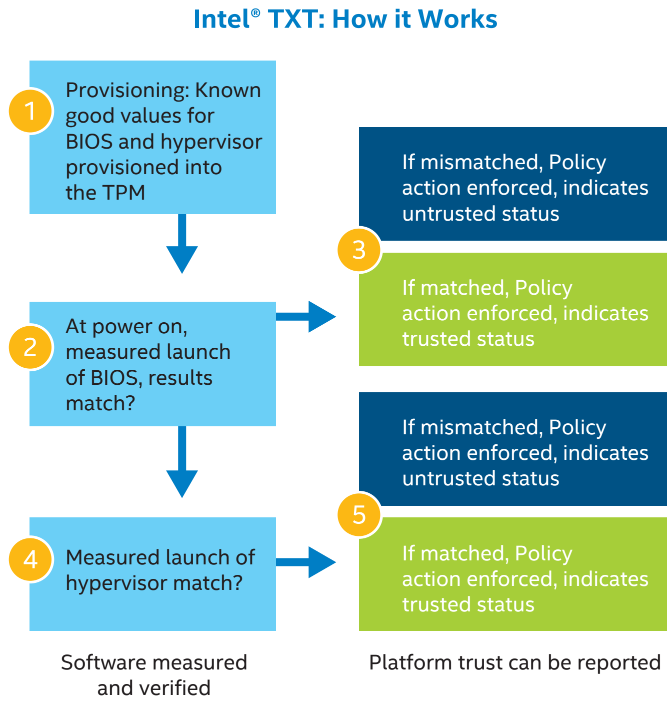

Intel® TXT: How it Works
1
Provisioning: Known good values for BIOS and hypervisor provisioned into the TPM
2
At power on, measured launch of BIOS, results match?
4
Measured launch of hypervisor match?
3
If mismatched, Policy action enforced, indicates untrusted status
If matched, Policy action enforced, indicates trusted status
5
If mismatched, Policy action enforced, indicates untrusted status
If matched, Policy action enforced, indicates trusted status
Software measured and verified
Platform trust can be reported

Figure 2. Intel® Trusted Execution Technology workflow

For secure workload and virtual machine (VM) placement in trusted compute pools, the VNF and orchestrator have the ability to demand "secure" processing resources from the VIM. The workload placement policy can include a requirement to select an infrastructure that includes Intel TXT, to ensure an MLE. For example, the ETSI NFV-MANO defined[8] *platform_security_parameter* information element in the virtual deployment unit (VDU) descriptor enables a VNF to be deployed on suitably equipped platforms.

Additional information on Intel TXT can be found here: http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper..html

Intel® Cloud Integrity Technology

Intel CIT is a multi-hypervisor, multi-device, trust attestation, and verification solution for servers, clients, network, storage, and embedded devices. Intel CIT is a comprehensive attestation solution that leverages Intel TXT to provide "trust" visibility of the cloud infrastructure and enables compliance in cloud data centers. The solution leverages Intel technology to establish hardware root of trust and builds the chain of trust across hardware, OS, hypervisor, and asset tagging for location and boundary control. This enables service providers to trust the integrity of the servers, trust where the servers are located, control where VMs or Containers are distributed, trust the workloads, and encrypt and control the decryption of the workloads.

Intel CIT's ability to validate the authenticity of the platform, infrastructure, and virtualized workloads serves as a foundation to ensure a trusted virtualized network. For example, if the cloud vSwitch* is compromised, an unsafe network that is vulnerable to malicious attacks may result. Intel CIT records the boot-time environment to create a whitelist, measures OS, hypervisor, VMs, apps, and Open vSwitch (OVS), and compares the measurements with the whitelist to validate a trusted network stack and applications running on the stack.

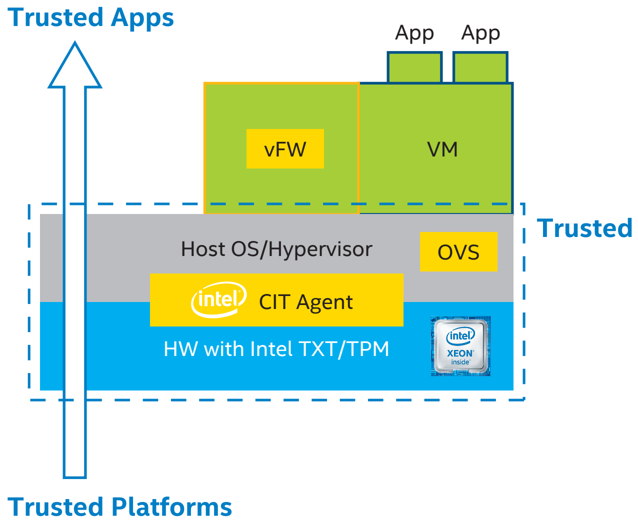


Figure 3. Intel® Trusted Execution Technology workflow

Hardware-based geography asset tags help control workload placement and migration. As shown in Figure 3, the platform trust and asset tag attestation information can be used by orchestrators and/or policy compliance management to ensure workloads are launched on trusted and location/boundary compliant platforms. Intel CIT provides the needed visibility and auditability of the infrastructure in both public and private cloud environments. As shown in Figure 4, boundary control policy can be set for workloads allowing or preventing workload deployment.

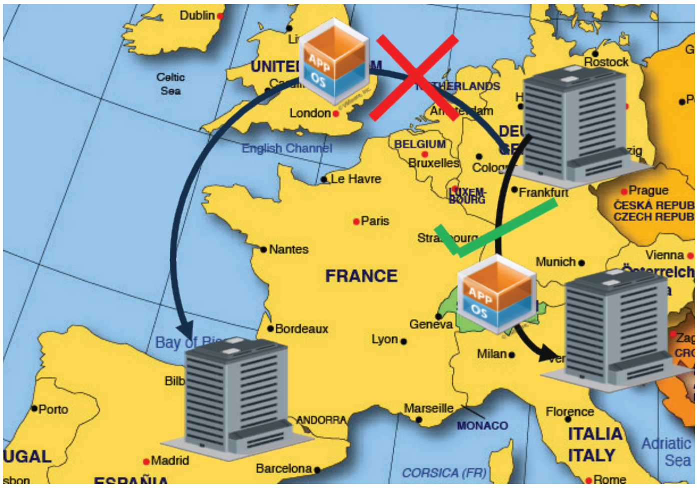


Figure 4. Trusted location and boundary control required for subscriber information

The Intel CIT trust attestation server provides a RESTful API interface for simple third-party integration. This provides the ability to tag and verify hosts with custom attributes or asset tags stored in the TPM and audit logging for all changes. Intel CIT enables the provisioning of asset tags to capable hosts, trusted placement, and the continuous monitoring of the chain of trust.

Additional information on Intel CIT and Open CIT can be found here:

http://www.intel.com/content/www/us/en/support/software/data-center-software/000006233.html

https://01.org/opencit

Intel® Clear Containers

The benefits of Container technology, such as lightweight, fast boot time, and resource efficiency, provide compelling reasons for Comms SPs to incorporate the technology as a means to address the overhead of an SDN/NFV environment. However, Containers are still an emerging technology, with Security concerns one of the major barriers to adoption that must be addressed and hardened. The shared resource aspect that makes Container technology so compelling also exposes some security vulnerabilities and attack surfaces that must be addressed to enable the use of the technology in wide-scale production deployments.

Intel is actively participating in Clear Linux*,[9] an open source initiative to address the security vulnerabilities associated with Containers and bridge the gap between VM-based and Container approaches. Clear Linux utilizes a thin hypervisor optimized for Intel® architecture to provide the benefits of VM security while leveraging Intel® Virtualization Technology (Intel® VT) to enable Container deployments to realize the promised performance benefits.[10]

As shown in Figure 5, Intel Clear Containers 2.0 provides the best of the VM workload and Container environments. The OS layer is shared transparently and securely from the host into the address space of each Intel Clear Container, which provides an optimal combination of high security with low overhead. Intel Clear Containers hardware-assisted Container isolation and security provide isolation for Containers from the host OS.

Additional information on Intel Clear Containers can be found here:

https://01.org/sites/default/files/page/vmscontainers_wp_final.pdf

https://clearlinux.org

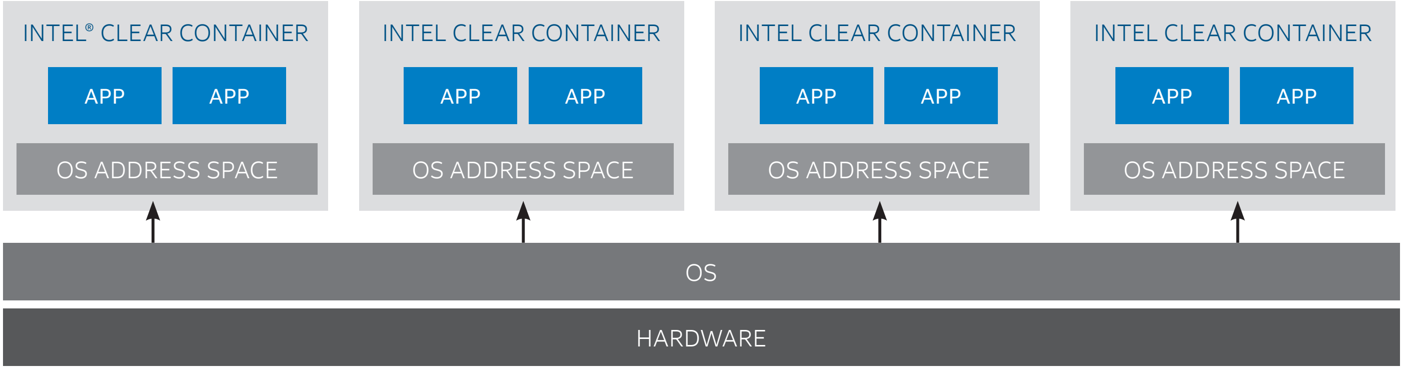


Figure 5. Intel® Clear Containers

Intel® Resource Director Technology

Intel RDT provides visibility and control over how shared resources such as last-level cache (LLC) and memory bandwidth are used by applications, VMs, and Containers.

Intel RDT enables Platform Quality of Service (PQoS) by providing control over shared platform resources using Cache Monitoring Technology, Cache Allocation Technology (CAT), Memory Bandwidth Monitoring (MBM), and Code and Data Prioritization (CDP). Virtualized environments using shared physical resources must account for multitenant scenarios, in which "noisy neighbors" may impact the performance of an application. Intel RDT identifies misbehaving applications and enables the capability to allocate a specific amount of cache to memory-intensive applications and ensure that the performance of other applications is not negatively impacted.

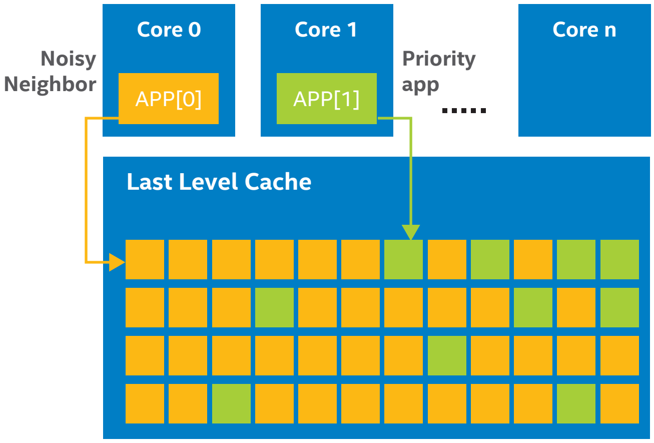


Figure 6. CAT defines LLC for class of service

There is also research underway to study the use of CAT to determine its effectiveness to address LLC-based attacks (see Figure 6). LLC is a shared resource by all the cores in the processor. This allows for potential side channel attacks whereby secret information in one VM may be extracted by another co-resident VM, even when VMs are scheduled on different cores.

CAT may potentially be used to provide a system-level protection mechanism to defend from side channel attacks on the shared LLC.[11] Further research and investigation is required to validate the use of standard Intel® processors with CAT technology to prevent LLC scraping. The results so far have been promising. Institute of Electrical and Electronics Engineers (IEEE) research efforts continue to delve into this area and provide examples of how CAT can be used to address LLC side channel attacks in cloud computing.[12]

Additional information on Intel RDT can be found here:

http://www.intel.com/content/www/us/en/architecture-and-technology/resource-director-technology.html

http://www.intel.com/content/www/us/en/communications/cache-allocation-technology-white-paper.html

Security Virtualization Workload Acceleration

Intel® QuickAssist Technology

Intel® QuickAssist Technology provides the security and compression acceleration capabilities used to improve performance and efficiency across the data center. Intel QuickAssist Technology enables service providers to increase platform efficiencies and optimize the use of the virtualized resources by offloading servers from handling compute-intensive operations, such as compression, cryptography, and key management.

Intel QuickAssist Technology provides service providers with the technology to ensure applications are fast, secure, and available. Intel QuickAssist Technology will also help Comms SPs scale virtualized network functions and improve the end-user experience. Some of these benefits include:

- Increased secure server throughput
- Real-time data compression benefits
- Less physical storage required
- Maximizes CPU utilization
- Enhances the ability to differentiate a specific solution.

Additional information on Intel QuickAssist Technology can be found here:

http://www.intel.com/content/www/us/en/embedded/technology/quickassist/overview.html

http://www.intel.com/content/www/us/en/ethernet-products/gigabit-server-adapters/quickassist-adapter-for-servers.html

Hyperscan Technology

Hyperscan[13] is a software pattern-matching library for optimized content inspection and performance for virtualized functions. Hyperscan pattern matching is ideal for applications that inspect large data volumes at high speeds. Hyperscan works transparently in any hypervisor environment and is OS independent so that it can be utilized by VNFs for optimal performance.

High-speed pattern matching security VNFs, including Intrusion Prevention (IPS), Antivirus (AV), Unified Threat Management (UTM), and Deep Packet Inspection (DPI), have been demonstrated to deliver order-of-magnitude performance benefits when using Hyperscan. For example, as captured in this briefing, Hyperscan has delivered performance benefits to Suricata*, an open source IDS/IPS.

Additional information on Hyperscan and example performance gains:

http://www.intel.com/content/www/us/en/communications/hyperscan-suricata-solution-brief.html

Intel® Processor Instructions

Intel® Advanced Encryption Standard New Instructions

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) accelerates the encryption of data in the Intel® Xeon® processor family and the Intel® Core™ processor family. Intel AES-NI provides cryptographic accelerations that reduce resource requirements for critical security workloads, such as SSL and IPSec. The horizontal aspect of virtualization, with workloads spanning from edge to cloud, benefits from Intel AES-NI (e.g., acceleration capabilities) as it makes the use of encryption more feasible.

Intel has developed a plug-in for the Linux kernel crypto framework, which is the module within the Linux kernel that manages cryptographic operations. This kernel enabling work has enabled applications, such as Openswan*, to take advantage of Intel AES-NI more easily. For more information concerning the implementation of IPSec using Intel AES-NI, please see this whitepaper:

http://www.intel.ie/content/dam/www/public/us/en/documents/white-papers/aes-ipsec-performance-linux-paper.pdf

Also Intel has developed a Multi-Buffer Crypto for IPsec Library, a set of functions that implement the computationally intensive authentication and encryption algorithms for IPsec. For more information, please see:

http://www.intel.ie/content/dam/www/public/us/en/documents/white-papers/fast-multi-buffer-ipsec-implementations-ia-processors-paper.pdf

Additional information on Intel AES-NI can be found here:

http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html

http://www.intel.com/content/www/us/en/enterprise-security/enterprise-security-aes-ni-white-paper.html

Galois-Counter Mode (GCM)

Galois-Counter Mode (GCM) is a block cipher mode of operation providing data security with AES encryption and authentication with universal hashing over a binary field (GHASH). The main usage of GCM is in the IPSec, TLS 1.2, and SSH protocols, with the greatest benefit for secure network communications. AES-GCM has been described as the best performing Authenticated Encryption combination among the NIST standard options.[14]

Ongoing performance improvements are expected in the future generation of Intel processor-based architecture. GCM adoption will continue to grow for encryption workloads due to performance improvements on Intel processor-based architecture, which utilize the highly optimized code that Intel has developed.

Additional information on GCM can be found here:

http://www.intel.com/content/www/us/en/intelligent-systems/network-security/enabling-high-performance-gcm.html

http://www.intel.com/content/www/us/en/processors/carry-less-multiplication-instruction-in-gcm-mode-paper.html

Supervisor Mode Execution Protection (SMEP)

Supervisor Mode Execution Protection (SMEP) is defined to prevent instruction execution from user memory pages while the CPU is in supervisor mode. SMEP enables hardware-based protection against privilege escalation attacks.

Supervisor Mode Access Protection (SMAP) is a CPU-based mechanism for user-mode address-space protection. It extends the protection that previously was provided by Supervisor Mode Execution Prevention (SMEP). SMEP prevents supervisor mode execution from user pages, while SMAP prevents unintended supervisor mode accesses to data on user pages. There are legitimate instances where the OS needs to access user pages, and SMAP does provide support for those situations.

Additional information on SMEP can be found here:

http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-vol-2b-manual.pdf

Open Security Controller for SDN

The security vulnerabilities of value-added services, which had previously been siloed across the edge, mobile core, and cloud data center, are now required to be addressed, or offered as a service, at any location in the cloud-based model. As a result, a comprehensive Security Management architecture that is aligned with the SDN/NFV architecture should be considered to mitigate and address the vulnerabilities in a hybrid environment in which services cover both physical and virtual infrastructure.

As shown in Figure 7, Intel's Open Security Controller uses bidirectional, notification-based APIs and provides a continuous brokering service between security VNFs and the virtual network to enable security functions to be automatically provisioned and configured in compliance with the policies established by the administrator.

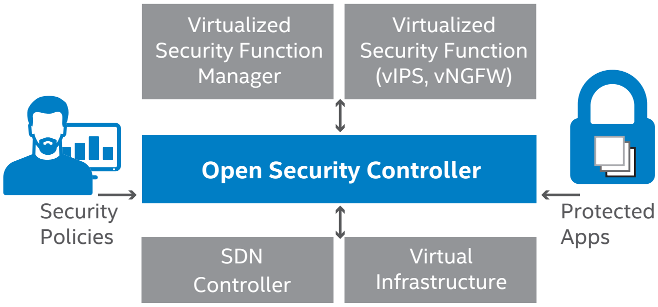


Figure 7. Open Security Controller

The inclusion of an Open Security Controller in the SDN/NFV architecture provides the following benefits:

- Orchestration for N security services across M virtualized data centers
- Abstracts the virtualization platform from the point solutions
- Provides cloud-agnostic management and orchestration of distributed security solutions
- Integrates with security VNFs from multiple vendors
- Provides non-disruptive delivery of security to workload VMs
- Seamlessly integrates with virtualized platforms and multiple SDN controllers

A centralized Open Security Controller framework provides the ability to abstract security infrastructure, inject services based on policy in workflow, and facilitate the addition of orchestrators and VNFs, with protection and remediation that is scalable across distributed data centers and distributed NFV/SDN architectures.

Additional information on the Open Security Controller can be found at:

http://www.intel.com/OSC

http://www.intel.com/content/www/us/en/software/open-security-controller/osc-datasheet.html

IDF16 Technical-Sessions:
CLDTC03 - Open Security Controller – Security Orchestration for a Software Defined Data Center

NFV Security Monitoring

SDN-NFV architecture deployment environments require a completely new methodology to gather telemetry for security monitoring. Some of the key aspects of security monitoring unique to NFV include:

- Multi-tenancy, multiple-control domains
- Shared and distributed infrastructure, east-west traffic
- Virtualized network overlays and service function chains
- Dynamic and automated services/VNF instantiations and migration

There are several industry efforts underway to better define the problem statements and target architectures to enable comprehensive NFV security monitoring solutions. One of the industry efforts in which Intel participates is the ETSI NFV security-working group. An initiative underway in this working group is the NFV Security Report for Security Management and Monitoring for NFV.

While this initiative is still at the drafting stage, it highlights several of the areas of focus and the possible architectures required to address security monitoring for NFV. The intent of the study is to drive toward the *establishment of holistic security policies and coherent enforcement of the policies across the lifecycle of the E2E network service in both virtualized and legacy networks.*[15] The report from the study produced the architecture shown in Figure 8.

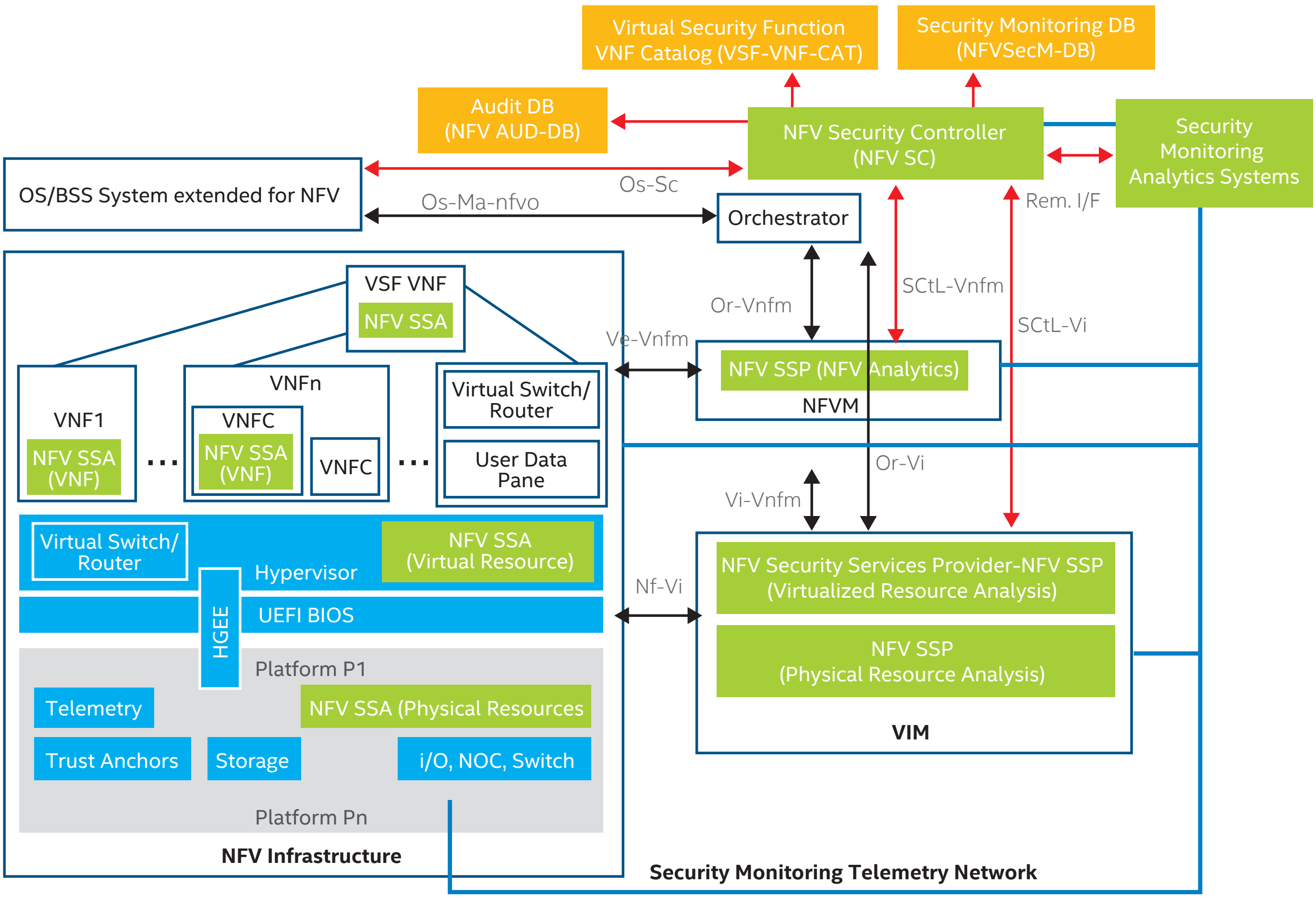

Virtual Security Function VNF Catalog (VSF-VNF-CAT)
Security Monitoring DB (NFVSecM-DB)
Audit DB (NFV AUD-DB)
NFV Security Controller (NFV SC)
Security Monitoring Analytics Systems
OS/BSS System extended for NFV
Os-Sc
Os-Ma-nfvo
Orchestrator
Rem. I/F
VSF VNF
NFV SSA
Or-Vnfm
SCtL-Vnfm
SCtL-Vi
Ve-Vnfm
NFV SSP (NFV Analytics)
NFVM
VNF1
NFV SSA (VNF)
. . .
VNFn
VNFC
NFV SSA (VNF)
VNFC
. . .
Virtual Switch/ Router
User Data Pane
Or-Vi
Vi-Vnfm
Virtual Switch/ Router
Hypervisor
NFV SSA (Virtual Resource)
HGEE
UEFI BIOS
Nf-Vi
NFV Security Services Provider-NFV SSP (Virtualized Resource Analysis)
NFV SSP (Physical Resource Analysis)
Platform P1
Telemetry
NFV SSA (Physical Resources
Trust Anchors
Storage
i/O, NOC, Switch
VIM
Platform Pn
NFV Infrastructure
Security Monitoring Telemetry Network

Figure 8. NFV Security Monitoring and Management Architecture

This architecture will be used to focus attention of the experts on the requirements to deliver capabilities such as security monitoring telemetry, pervasive traffic encryption, and anomaly detection/mitigation. Intel's involvement in the development of these standards will influence Intel's technology roadmap and accelerate delivery of solutions addressing these industry challenges.

Additional information on NFV security monitoring is available from several sources, including these sessions[16] from the 2016 Intel Developers Conference:

IDF16 Technical-Sessions:

- *Secure Traffic Monitoring for Virtualized Workloads in SDN & NFV Deployments*
- *Orchestrating Virtual Security Functions for Software Defined Infrastructure*

Additional Intel Technologies for Platform Security

Note: *This section provides links and information to additional Intel technologies that support and contribute to platform security. Although these technologies are currently used in other domains the work is underway to understand and apply these technologies in the SDN/NFV environment. Future versions of this document will reflect these updates.*

Intel® Software Guard Extensions

Intel® Software Guard Extensions (Intel® SGX) are Intel instruction set extensions that are used to protect select code and data from disclosure or modification. Through the use of "enclaves," which are protected areas of execution, the application code and application data are encrypted in hardware memory. Access to an enclave is only by special instructions and software made available to developers via the Intel SGX SDK. The Intel SGX SDK is a collection of APIs, libraries, documentation, sample source code, and tools for software developers (see Figure 9).

While Intel SGX research continues to be an area of focus, one of its key target benefits, as shown above, is keeping the application data protected even when the BIOS, VMM, OS, and drivers are compromised. The goal is to keep an attacker with full execution control over the platform at bay.

Additional information on Intel SGX can be found at:

https://software.intel.com/en-us/sgx

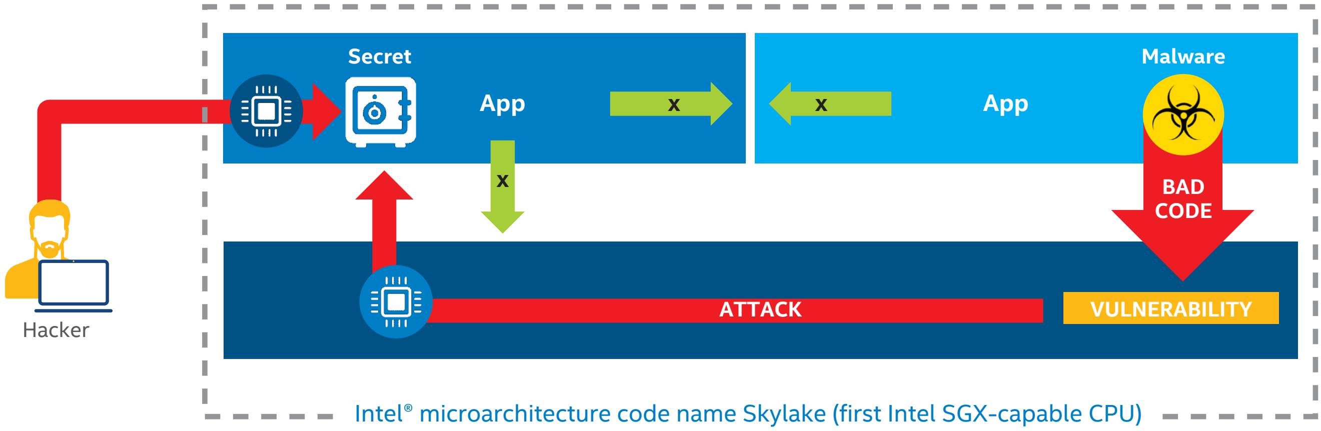
FPGA Acceleration For Security

Field Programmable Gate Arrays (FPGA) and System on a Chip (SoC) address multiple markets with different threat profiles. The future architecture for FPGA and SoC will address newer Internet of Things (IoT) and data center profiles, including virtualization. The ability to apply FPGA acceleration in a virtualized environment is promising, and subsequent versions of this document will highlight those capabilities.

For current information, refer to the following publicly available information:

https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/wp/wp-01252-secure-device-manager-for-fpga-soc-security.pdf

Intel® SGX: CPU-enhanced Application Security


Secret
App
x
x
x
App
Malware
BAD CODE
Hacker
ATTACK
VULNERABILITY
Intel® microarchitecture code name Skylake (first Intel SGX-capable CPU)

Empowering Developers to Better Protect Code and Data

Figure 9. Intel® Software Guard Extensions – CPU Enhanced Application Security

Intel® Platform Trust Technology

Intel® Platform Trust Technology (Intel® PTT) is a platform functionality for credential storage and key management. Intel PTT supports hard-drive encryption and the firmware TPM. Intel PTT is an integrated solution in the Intel® Management Engine for 4th generation Intel® Core™ processors with ultra-low TDP (Thermal Display Power) platforms.

Additional information on PTT:

http://www.intel.co.za/content/dam/www/public/us/en/documents/white-papers/enterprise-security-platform-trust-technology-white-paper.pdf

Boot Guard

Boot Guard is hardware-based boot integrity protection provided on Intel Core processors that prevents unauthorized software and malware takeover of boot blocks critical to a system's function. Intel PTT provides an added level of platform security based on hardware for a secure boot sign and verification solution.

Configurable boot types include Measured Boot and Verified Boot. Measured Boot measures the initial boot block into the platform storage device, such as TPM or Intel PTT). Verified Boot cryptographically verifies the platform initial boot block using the boot policy key.

Additional information on Boot Guard can be found at:

http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/4th-gen-core-family-mobile-brief.pdf

UEFI Secure Boot

Unified Extensible Firmware Interface (UEFI) Secure Boot helps a computer resist attacks and infection from malware. UEFI Secure Boot with the UEFI architecture checks the signatures (that is, signed cryptographic digests) or hash of all UEFI modules, as they are loaded. If the signature check fails, the boot stops.

Secure boot detects tampering with boot loaders, key OS files, and unauthorized option ROMs by validating their digital signatures. Detections are blocked from running before they can attack or infect the system. Code with valid credentials gets through the gate and executes, while code that has bad credentials, or no credentials, is blocked at the gate and rejected.

Additional information on UEFI Secure Boot can be found at:

http://www.intel.com/content/www/us/en/architecture-and-technology/unified-extensible-firmware-interface/efi-specifications-general-technology.html

Next steps

- To learn more about the security technologies mentioned in this paper, please follow the links.
- To learn more about Intel's technology for NFV, attend the courses available in the Intel® Network Builders University at **https://networkbuilders.intel.com/university**.
- To learn more about Intel Network Builder partners for NFV products, visit **https://networkbuilders.intel.com/solutionscatalog**.
- To build a test bed using the Intel® Open Network Platform Reference Architecture, download the documentation at **https://01.org/packet-processing/intel%C2%AE-onp**.
- To get the best security in your NFV systems, specify Intel CIT in your infrastructure and VNF procurements.
- To get the highest performance from your NFV systems, specify compatibility with the Data Plane Development Kit in your infrastructure and VNF procurements.
- To get the highest return on investment from your NFV systems, specify use of Enhanced Platform Awareness in your orchestration, infrastructure, and VNF procurements.

[1] http://www.telcotransformation.com/author.asp?section_id=396&doc_id=724401

[2] http://www.fiercetelecom.com/telecom/at-t-s-donovan-2016-a-critical-year-virtualizing-our-network

[3] http://www.lightreading.com/nfv/nfv-strategies/verizon-launches-virtual-network-services/d/d-id/724905

[4] https://www.business.att.com/enterprise/Family/network-services/network-functions-on-demand/

[5] http://www.newipagency.com/document.asp?doc_id=719010&site=thenewip

[6] https://www.opnfv.org/news-faq/press-release/2016/06/survey-reveals-93-percent-network-operators-view-opnfv-important

[7] ETSI NFV SEC001, Published Oct'14, SEC013, SEC009, SEC008, SEC010

[8] http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf

[9] https://clearlinux.org

[10] http://thenewstack.io/securing-containers-intels-clear-containers/

[11] http://www.intel.com/content/www/us/en/communications/cache-allocation-technology-white-paper.html

[12] https://www.computer.org/csdl/proceedings/hpca/2016/9211/00/07446082.pdf

[13] https://01.org/hyperscan

[14] https://crypto.stanford.edu/RealWorldCrypto/slides/gueron.pdf

[15] Draft ETSI GW NFV-SEC 013 v0.0.1 (2015-11)

[16] http://myeventagenda.com/sessions/0B9F4191-1C29-408A-8B61-65D7520025A8/14/5

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's web site at www.intel.com.