Integrated Solutions for Trusted Clouds and SDI

Steve Orrin
Federal Chief Technologist
Intel Corp

Shawn Wells
Chief Security Strategist
Red Hat Public Sector
In the next 45 minutes . . .

- Modern challenges for security and compliance in cloud stacks
- Building block technologies: hardware & software
- Step through reference designs
- What’s coming next?
  - SDN, SDS, containers, PaaS/SaaS, Audit as a Service
- Demos!
Key Security Challenges

- Attacks on the Infrastructure
- Co-tenancy Threats
- Building & Enforcing Trust

No physical boundaries.  
*Do you know where your workload/data is located?*

Lack of Visibility to the Integrity of Infrastructure.  
*How do you know your workloads are running on compliant infrastructure?*

Attacks are moving down in the stack.  
*How do you establish root of trust in h/w?*
Compliance & Regulatory Challenges

- Achieving audit visibility
- Commingled regulatory environments
- Continuous monitoring
- Data use
Building Blocks of Trustworthy Clouds

- Create a chain of trust rooted in hardware that extends to include the hypervisor
- Provide visibility for compliance and audit
- Use trust as part of the Policy Management for Cloud Activity
  - Trust as part of the VM Migration and Dynamic Provisioning Policies
- Server tagging for richer policy decisions
- Leverage infrastructure capabilities/services to address data protection requirements
When using a cloud, the tenant is not in control of their physical infrastructure. How do they:

- Verify provisioning of the infrastructure?
- Trust where servers are located?
- Control where VMs are distributed?
- Support data sovereignty?
- Implement granular controls?
- Audit policy configuration?
- Prove compliance to industry and regulators?
Building Blocks
Building Block Technologies

Hardware
- TXT, AESNI, DRNG, CryptoNI

Software
- Linux, KVM, OpenStack, CloudForms, Ceph, VMWare (VCenter, VSphere, ESXi), OpenCIT, Hytrust, Cloud Raxak
How HW Root of Trust is established

Trusted Execution Technology

Trusted Launch
Enables isolation and tamper detection at boot-time

Compliance
Hardware-based verification for compliance

TPM
BIOS
Chipset
VT
Flash
VMM/OS
Hardware Features for Data Protection

AES HW Acceleration with AES-NI
- Ubiquitous Data Protection with Cryptographic Acceleration
  - AES-NI allows significant performance at a lower price-point, no custom hardware

HW DRNG
- Better Keys and Simulations with On-Board Digital Random Number Generator
- Stronger encryption keys
  - High degree of entropy provides quality random numbers for encryption keys and other operations
  - DRNG solves the problem of limited entropy in virtual platforms

Secure transactions on Internet and Intranet
Application-level encryption for automation and granularity

Full-disk encryption protects data on hard disks
Instructions for Asymmetric Cryptography Acceleration
ADOX/ADCX

Extension of ADC (Add with Carry) instruction for use in large integer arithmetic (integers MUCH larger than 64b); one common use is Public Key cryptography (e.g. RSA)

- ADOX - Unsigned Integer Addition with carry-in/out using the Overflow Flag
- ADCX - Unsigned Integer Addition with carry-in/out using the Carry Flag

Performance improvements are due to two parallel carry chains being supported at the same time

<table>
<thead>
<tr>
<th>Instruction Sequence</th>
<th>Instruction Sequence</th>
<th>Instruction Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>mov r0, [r1+100h]</td>
<td>mov r0, [r1+100h]</td>
<td>mov r0, [r1+100h]</td>
</tr>
<tr>
<td>mov r0, [r1+100h]</td>
<td>mov r0, [r1+100h]</td>
<td>mov r0, [r1+100h]</td>
</tr>
<tr>
<td>add r1, r0</td>
<td>add r1, r0</td>
<td>add r1, r0</td>
</tr>
<tr>
<td>adc r0, 0</td>
<td>adc r0, 0</td>
<td>adc r0, 0</td>
</tr>
<tr>
<td>mov r1, r0</td>
<td>mov r1, r0</td>
<td>mov r1, r0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

ADOX/ADCX Used with MULX Can Substantially Improve Public Key Encryption Code Performance
Trusted Compute Pools

Addresses critical needs in virtualized & cloud use models
- Provides control to ensure only trustable hypervisor is run on platform
- Protecting server prior to virtualization software boot
- Launch-time protections that complement run-time malware protections
- Compliance Support

Control VMs based on platform trust
- Pools of platforms with trusted hypervisor
- VM Migration controlled across resource pools
- Similar to clearing airport checkpoint and then moving freely between gates
OpenCIT (Open Cloud Integrity Technology)
Platform Trust, Trusted Compute Pools

- Uses Intel’s TXT and the Platform’s TPM to verify the integrity of a platform (BIOS, OS, hypervisor) against a “known good state” or “whitelist” at boot time
- Helps create logical groupings (pools) of trusted systems, separates them from untrusted systems
- Enables:
  - **Visibility**: Identify trusted platforms vs. untrusted
  - **Control**: Set policy that only allows workloads to run on trusted servers
  - **Monitoring**: Trust-based policies can be automatically tracked
  - **Compliance**: Trust information can be delivered to audit logs
- Available at [https://01.org/opencit](https://01.org/opencit)
- Delivered via OpenStack or integrated into Policy & Compliance products, e.g. HyTrust Cloud Control

Use Model 1: Trusted Launch
Attestation provides information about platform trust to improve response to malware threats

Use Model 2: Trusted Compute Pools
Attestation provides information to inform us of which systems are trustworthy for hosting our workloads

Use Model 3: Compliance
Attestation allows us to verify platform trust for comparison against policy and use in audit
OpenCIT (Open Cloud Integrity Technology)
Trusted Location and Boundary Control

➢ Hardware-based Geo- and Asset Tags help control workload placement and migration
➢ Tags are securely stored in TPM, tag integrity is assured
➢ Location Boundary Control policy can be set for a workload, allowing or preventing its deployment
➢ This helps address and prove data sovereignty requirements
➢ Delivered via OpenStack or Policy & Compliance product, e.g. HyTrust Cloud Control

Addresses top cloud concerns:
• Visibility and Control of Workload Location
• Auditability and Regulatory Compliance
Attested Server Tagging & Trusted Geo-location in the Cloud

- Many Trusted Compute Pools use cases also require:
  - GEO tagging
- Regulatory Compliance Requirements:
  - EU data protection directives (95/46/EC)
  - FISMA (geo-tag)
  - Payment Card Industry (PCI-DSS) (asset tag)
  - HIPPA (Asset Tag)

A PoC of the NIST IR 7904 solution is at the NIST National Cyber Center of Excellence (NCCOE) in Rockville, MD

NIST IR 7904 – USG recommendation for “Trusted Geolocation in the Cloud”

- Trusted resource pool based on hardware-based secure technical measurement capability
  - Platform attestation and safer hypervisor launch - Provide integrity measurement and enforcement for the compute nodes
  - Trust-based secure migration - Provide geolocation measurement and enforcement for the compute nodes
OpenCIT (Open Cloud Integrity Technology)
Workload Integrity and Confidentiality with OpenStack

- Extend trust from BIOS to workload
  - Boot-time integrity of workload
  - Workload can be a VM or container
  - Integrated with OpenStack
- Enterprise Ownership and Control
  - Encrypt workload before moving it to cloud
  - Own and manage the encryption keys
  - Only release keys to CSP after integrity check succeeds
  - This ensures verifiable end-to-end protection
- Can be applied to storage and network workloads too
"Security in the cloud is paramount and Virtustream has adopted some of Intel technologies around security including Intel TXT." - Don Whittington, VP & CIO, Florida Crystals

"Hardware-enhanced security provided by Intel TXT is critical to protect our sensitive data and was key in our selection of Virtustream for cloud services." - Joh F. Hill, CIO, Veyance Technologies

DuPont deployed Intel TXT to ensure that the computing pools remained trusted, based on the original configurations across both Linux and Windows operating environments.

“Security in the cloud is paramount and Virtustream has adopted some of Intel technologies around security including Intel TXT.” - Don Whittington, VP & CIO, Florida Crystals

"Hardware-enhanced security provided by Intel TXT is critical to protect our sensitive data and was key in our selection of Virtustream for cloud services.” - Joh F. Hill, CIO, Veyance Technologies
Reference Designs
Real World Solutions

- Private Cloud Implementations
  - VMWare + Intel + HyTrust
  - Intel + Red Hat (RHEL/OpenStack/CloudForms/Ceph)

- Commercial Solution Providers (CSP’s)
  - IBM Softlayer (w/VMWare + Intel + HyTrust)
  - CSRA (w/Intel + Red Hat)

- Hyper Converged Secure SCI
  - BlackBox + NEC + Red Hat + Intel
Intel + Vmware + HyTrust: Secure Private/Hybrid Cloud

**Hardware with:**
- Root-of-Trust (TXT)
- Crypto acceleration (AES-NI)

**VM and Data Encryption with:**
- Fully automatic key management
- Zero-downtime encryption/rekey
- HW-speed crypto (using Intel AES-NI)
- Boundary controlled decryption (using Intel TXT)

**Policy-based controls with:**
- Secure Governance of V-Admins
- V-Infrastructure hardening
- Compliance logging and full audit
- Physical host trust-attestation
- Geo and logical boundary enforcement (using Intel TXT)
The Road to a Secure, Compliant Cloud
A trusted infrastructure with a solution stack from Intel®, IBM Cloud SoftLayer, VMware, and HyTrust

Elements of a trusted cloud infrastructure

- HyTrust Cloud Control
- HyTrust Data Control
- VMware vCenter management server
- VMware ESXi hypervisor
- IBM Cloud SoftLayer cloud infrastructure
- Bare-metal servers
- Intel® Trusted Execution Technology (Intel® TXT)

Telecommunications:
- Establish policies, auditing, reporting, and perform encryption
- Manages virtual machines and ESXi hosts
- Allows user to install their own operating systems, hypervisors, applications as needed
- Ensures trust from the hardware level up

Measurements of launch environment are stored in hardware

- Software-based tags
- Hardware-based tags
- Hardware-based tags for physical location of servers
- Management virtual appliances
- HyTrust Cloud Control (HTCC)
- HyTrust Data Control (HTDC)

Geo-fencing: Restrict workloads to specific servers within a trusted pool

- Accounting workloads allowed
- Sales workload
- Accounting to separate workloads
- Geo-fence sales workloads
- Sales workloads allowed
Cloud Service Models

FedRAMP

IaaS  PaaS  SaaS

APPLICATION
APPLICATION PLATFORM  (JBoss, PHP, Ruby, etc)
OPERATING SYSTEM  (RHEL)
VIRTUALIZATION  (RHEV)
HARDWARE  (x86 w/ TXT)
STORAGE  (RHS)

Managed and Controlled by Customer (IT, Dev, or User)
Automated and Managed by the Public or Private Cloud Offering

Increased Control
Increased Automation
Collectively delivering a highly performant, secure hyper-converged infrastructure appliance that is built for web-scale environments with NexGen technology in OpenSource environment.

- Provide a comprehensive cloud management tool that allows management, metering and charge-back for bi-modal (traditional mode-1 and agile, web-scale mode-2) environments; across on-premise private cloud as well as lower security public cloud offerings from Amazon and Microsoft.

- Provide agility and flexibility to the data center resources with the ability to dynamically reallocate resources with respect to compute, storage and networking.

- Ability to replace expensive legacy high-end networking and storage with cost effective infrastructure at a fraction of the price without sacrificing the intelligence and benefits.

- Support for Multi-Layer Security in a multi tenant cloud
Demos!
Demo #1: Automated Security Scanning

http://docs.openstack.org/sec/

https://www.open-scap.org/
### Demo #2: OpenCIT (1 / 2)

#### Trust Dashboard

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Asset Tag Status</th>
<th>BIOS Trust</th>
<th>VMM Trust</th>
<th>Platform Trust</th>
<th>Updated</th>
<th>Trust Status</th>
<th>Trust Report</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL7</td>
<td>redhat.gp</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>2016-08-26</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WIN-PG18A7SEMIU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2016-08-26</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Trust Report

<table>
<thead>
<tr>
<th>PCR Name</th>
<th>PCR Value</th>
<th>WhiteList Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>891eb0b556b830f1c10f3a6644345e348f91</td>
<td>981B5B56B830F1C103F8F646345E348F91</td>
</tr>
<tr>
<td>17</td>
<td>bfc3f6d7940e9281a3ebdf4e0412869a3f55b8</td>
<td>BFC3F6D7940E9281A3EBDF4E0412869A3F5558</td>
</tr>
<tr>
<td>18</td>
<td>2d961a16d2e367557471c8b1ed93a95b213b2</td>
<td>D961A16D263E67557471C8B1E93A95B213B2</td>
</tr>
<tr>
<td>19</td>
<td>0cc01be9c3e2e96efa74beca0a9758a8e0f2c9a0</td>
<td>C01BE9C3E2E96EFA74BEC0A9758A8E0F2C9A0</td>
</tr>
</tbody>
</table>

![Trust Dashboard Screenshot](image-url)
Demo #2: OpenCIT (2 / 2)

Key Features
- Establish chain of trust of BIOS, firmware, OS kernel & hypervisor by verifying against configured good values (whitelists)
- Ability to tag/verify hosts with custom attributes stored in TPM
- OpenStack & VMWare integration
- Mutual SSL authentication
- RESTful API
- User defined TLS policies
Roadmap
Roadmap: Security Enhanced OpenStack

- **Encryption & Key Management**
  - TLS/SSL for external services
  - Fernet token support
  - Maturing Single Sign On
  - Domain focused & implied roles

- **Governance & Risk Management**
  - Barbican [fully supported]
  - Custodia [TP1]
  - Cinder encrypted volumes
  - Infrastructure & virtualization hardened images
  - CloudForms based Governance and Risk Management
  - Attestation/TXT [TP1]

- **OS Security Documentation**
  - More coverage of TLS/SSL for internal services
  - Maturing Federation services

- **Infrastructure & Virtualization**
  - Barbican [fully supported]
  - Custodia [TP1]
  - Cinder encrypted volumes
  - Infrastructure & virtualization hardened images

- **Identity and Access Management**
  - More coverage of TLS/SSL for internal services
  - Maturing Federation services

- **Change Control & Configuration Management**
  - Barbican [fully supported]
  - Custodia [TP1]
  - Cinder encrypted volumes
  - Infrastructure & virtualization hardened images

- **Component & Interface Security**
  - Barbican [fully supported]
  - Custodia [TP1]
  - Cinder encrypted volumes
  - Infrastructure & virtualization hardened images

- **Interoperability & Portability**
  - Barbican [fully supported]
  - Custodia [TP1]
  - Cinder encrypted volumes
  - Infrastructure & virtualization hardened images

Control group coverage legend:
- Security Enhanced OSP
- DESIGN
- BUILD
- MANAGE
- RUN
- ADAPT
- early
- good
- strong

( projected default product coverage for various compliance framework technical controls )
Encryption and Key Management

Barbican - secure storage, provisioning and management of secrets

Secrets Management
- As a service used by many components, Barbican stores, provisions and manages secrets such as:
  - private keys
  - certificates
  - passwords
  - SSH keys

Secrets Storage

Encryption mechanisms and backends
- Network Security Services (NSS) support via Dogtag.
- Network Hardware Security Modules (SafeNet) and Key Management Interoperability Protocol (KMIP) support

Foundational for enhanced security
Unblocks security for other components
Will include HSM support long term
What’s coming next

- SDN, SDS, Containers, PaaS/SaaS, Audit as a Service
Cloud Security begins with trust and visibility enabled by hardware and delivered by the infrastructure

- Intel is driving hardware assisted security into the ecosystem of OEMs, ISVs, and CSPs
- Red Hat enables the technologies in Linux and OpenStack for private, hybrid, and public cloud

The risks and threats to the Cloud can be mitigated and managed

- But it takes an ecosystem of software, hardware, and service providers
Call to Action

Work with your vendors and CSPs
- Require security and trust for your workloads and data
- Require visibility and the necessary feeds and monitoring to achieve compliance
- For Private and Hybrid use cases, implement your policies for workload and data protection/control and then enforce them via orchestration
- Make platform/HW trust a requirement on your service providers and supply chain

Verify, then Trust, then Verify again
- Validate that controls are configured correctly and generating the necessary ‘evidence’ (logs, reports, attestation of trust, ....)
- Continuously validate trust level and residency

What should be Next?
- What architectures and configurations should Industry tackle next?
- Where else is trust and secure orchestration needed?
Contact Us

Steve Orrin
Federal Chief Technologist, Intel Corp
steve.orrin@intel.com

Shawn Wells [LinkedIn]
Chief Security Strategist, Red Hat Public Sector
shawn@redhat.com
Legal Disclaimers

- 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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENCE IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

- 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 go to: http://www.intel.com/design/literature.htm

Intel, the Intel logo, Intel Xeon, Xeon logo, and the Look Inside. logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2017 Intel Corporation. All rights reserved.
• Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Go to: Learn About Intel® Processor Numbers [http://www.intel.com/products/processor_number](http://www.intel.com/products/processor_number)

• Some results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.

• Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

• Intel does not control or audit the design or implementation of third party benchmarks or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmarks are reported and confirm whether the referenced benchmarks are accurate and reflect performance of systems available for purchase.

• Relative performance is calculated by assigning a baseline value of 1.0 to one benchmark result, and then dividing the actual benchmark result for the baseline platform into each of the specific benchmark results of each of the other platforms, and assigning them a relative performance number that correlates with the performance improvements reported.

• SPEC, SPECint, SPECfp, SPECrate, SPECpower, SPECjbb, SPECComp, SPEC MPI, and SPECjEnterprise® are trademarks of the Standard Performance Evaluation Corporation. See [http://www.spec.org](http://www.spec.org) for more information.

• TPC Benchmark, TPC-C, TPC-H, and TPC-E are trademarks of the Transaction Processing Council. See [http://www.tpc.org](http://www.tpc.org) for more information.

• Intel® Advanced Vector Extensions (Intel® AVX)* are designed to achieve higher throughput to certain integer and floating point operations. Due to varying processor power characteristics, utilizing AVX instructions may cause a) some parts to operate at less than the rated frequency and b) some parts with Intel® Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you should consult your system manufacturer for more information.

• No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware and/or software optimized to use the technologies. Consult your system manufacturer and/or software vendor for more information.

*Intel® Advanced Vector Extensions refers to Intel® AVX, Intel® AVX2 or Intel® AVX-512. For more information on Intel® Turbo Boost Technology 2.0, visit [http://www.intel.com/go/turbo](http://www.intel.com/go/turbo)