Agenda

- Background
- Architecture
- Implementation Details
- Summary
Background
Challenges

- Reduced physical control, visibility
- Increased multi-tenancy
- Reduced effectiveness/efficiency of existing security toolbox
- Increased attack surface

Datacenter Virtualization Drives New Security Needs

Traditional Data Center

Mfg
HR

Virtualized and Private Cloud Data Center

Mfg
HR
Sales
VMM

Public Cloud Data Center

Company A
Company B
Company C

IT Security Policy

Challenges

IT Pro survey of key concerns:

61% Lack of visibility inhibiting private cloud adoption

55% Lack of control over data key concern for public cloud adoption

57% Avoid putting workloads with compliance mandates in cloud

1 source: McCann “what's holding the cloud back?” cloud security global IT survey, sponsored by Intel, May 2012
**Trusted Compute Pools Usage Models**

1. **Trusted Boot**: Hardware-based root enforcement of launched environments – reduces malware threat

2. **Trust Based Policy Enforcement**: Control VMMs based on platform trust (and more) – better data protection

3. **Infrastructure Audit and Compliance Reporting**: Hardware-enforced compliance reporting

**Trusted Compute Pools**: Helps meeting new security needs
Trusted Compute Pools Key Components

- Hardware assisted platform integrity measurement
  - H/W platforms with Intel® Trusted Execution Technology support
  - tboot + OS/VMM supporting measured boot based on Intel® TXT
- Remote attestation service providing platform trustworthiness based on platform integrity
  - OpenAttestation providing attestation service & host agent
- Management tools enhanced with Trusted Compute Pools feature
Intel® Trusted Execution Technology (Intel® TXT)

- Enables isolation and tamper detection in boot process
- Complements runtime protections
- Reduces support and remediation costs
- Hardware-based trust increases assurance for compliance
- Trust status usable by security and policy applications to control workload
- Trusted Boot (Tboot): Pre-kernel module using TXT to perform measured and verified launch of OS kernel/VMM.

Hardens and Helps Control the Platform
OpenAttestation (OAT)

- SDK for managing host integrity verification.
- Use TCG-defined remote attestation protocol.
- Target at cloud and enterprise management tools.

https://github.com/OpenAttestation/OpenAttestation.git

- Open Source project established by Intel in Q1’12, v1.6 released in Q4’12, v2.0 released in Q3’13
OAT Architecture

Attestation Server (Tomcat)

Privacy CA

Appraiser

Whitelist API

Installation and provisioning scripts, CLI tools

Host Agent API

Query API

SDK Components

DB(mysql)

Whitelist Table

Hosts Table

Hardware/TXT

Hypervisor / tboot

OS

App

App

App

OAT provides standard RESTful API interfaces

- Privacy Certificate Authority (Privacy CA), Appraiser, Host Agent are Java*
- Host Agent accesses TPM through TrouSerS
oVirt Components Requiring Changes

- Postgres
- AD
- IPA

- Shared Storage: FC/iSCSI/NFS
- Local Storage

- Guest agent
- Linux VM
- Win VM
- libvirt
- VDSM
- Host | Node

- oVirt Engine: Java
- REST

- Admin Portal: gwt
- SDK/CLI: python
- User Portal: gwt

- Linux/Windows client
Statically Partitioning

Add host:
User specifies ::
cluster = “Trusted Cluster”
Key advantages

• No migration support issue

• No additional scheduling performance lost
Implementation Details
Status

- Feature page: [http://www.ovirt.org/Trusted_compute_pools](http://www.ovirt.org/Trusted_compute_pools)
- Work started since Dec 2012, finished by Aug 2013
- Available in oVirt 3.3 (Sep 16, 2013)
Frontend:
**Backend**

- Add attestation check logic in "InitVdsOnUpCommand.java"
  - Trusted host “Up” and untrusted host put as non-operational status
  - Expected trigger conditions:
    - Add a host into a trust cluster
    - Host rebooted
  - Call SetNonOperationalVdsCommand with a new NonOperationalReason
    - Migrate all VMs from the host and then set it non-operational.

- Add aggregated attestation check in Backend.Initialize()
  - Fire a one-time background request from this method to avoid blocking it
  - Do attestation by stages:
    - Configurable max number of attested hosts in stages:
      - **Stage 1:** FIRST_STAGE_QUERY_SIZE, 10 as default
      - **Stage N:** SECOND_STAGE_QUERY_SIZE, 20 as default
Database

- `vds_groups` table: add a new field, `trusted_service`. 
RESTful API

- Key relevant modification includes `api.xsd` and `VmMapper.java`

```bash
curl -v -u "admin:password"
  -H "content-type: application/xml"
  -d '<cluster><name>my_cluster</name>
      <trusted_service>true</trusted_service>
  </cluster>'
'http://engine.***.com:80/api/cluster'
```
OVF

- A new flag in OVF: trusted_service
  Record whether the VM is exported from a trusted cluster

- Key relevant classes:
  OvfTemplate{Reader|Writer}.java
  OvfVm{Reader|Writer}.java

- Alert for importing a 'trusted' VM into an untrusted cluster
  - Alert via printing event log
Future Work

• High Availability solution
• Etc.
Summary
Trusted Compute Pools Feature in oVirt Summary

- Trusted Compute Pools provides a way for Cloud/Datacenter administrator to deploy VMs on trusted hosts for data protection & service differentiation.

- Intel® TXT provides hardware support for Trusted Compute Pools usage.

- Trusted Boot (tboot) and OpenAttestation (OAT) are two key components for the deployment of Trusted Compute Pools.
Q&A
Backup
User specifies ::
trusted_host_flag = true

Dynamically Filtering

Scheduler
oVirt Engine
Attestation Broker
Cache

Host A
Host B
Host C

Attestation Server
Privacy CA
Appraiser
Whitelist API
Query API
Whitelist DB
Host Agent API

Host agent
OS
Hypervisor
HW/TXT

Host A
Host B
Host C

Attestation Broker
Cache

Attestation Service
Key issues

- Migration support
- Scheduling performance
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. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

Intel may make changes to specifications and product descriptions at any time, without notice. 

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. 

Intel, processors, chipsets, and desktop boards 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. 

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security 

Intel, Intel logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. 

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

Copyright © 2013 Intel Corporation. All rights reserved.