Adding Xen vTPM support to OpenStack Project Proposal

Daniel Pereira, Gerardo Ravago, Nick Morrison, Yuxin Cao

1. Vision and Goals of the Project:

Currently, when using IaaS providers, users are unable to establish trust prior to placing their secrets (keys, customer data, etc.) into the cloud. A solution to this problem would be to utilize cryptographic hardware common on many laptop computers. A trusted platform module, or TPM, is a hardware cryptographic co-processor used to secure secrets. Xen currently offers a virtualized instance of this hardware, known as a vTPM. Our vision is to allow end-users to utilize the cryptographic capabilities of a vTPM to securely provision secrets into their OpenStack instances. Our high level goals for this solution are as follows:

- Seamlessly integrate Xen (with vTPM) with OpenStack
- Streamline process such that spinning up a Nova instance also spins up and binds a vTPM
- Store the ID associating the instance with its matching vTPM
- Integrate existing Lincoln Labs software allowing cloud users to be able to securely provision secrets into their VMs
- Make above process invisible to user and provider

Users/Personas Of The Project:

- OpenStack User
    - Users of OpenStack should be able to set vTPM usage from the command line (if possible integrate into OpenStack Horizon dashboard)
- OpenStack Cloud Provider
    - Integration should be seamless - vTPM creation and matching should be fully automated

2. Scope and Features Of The Project:

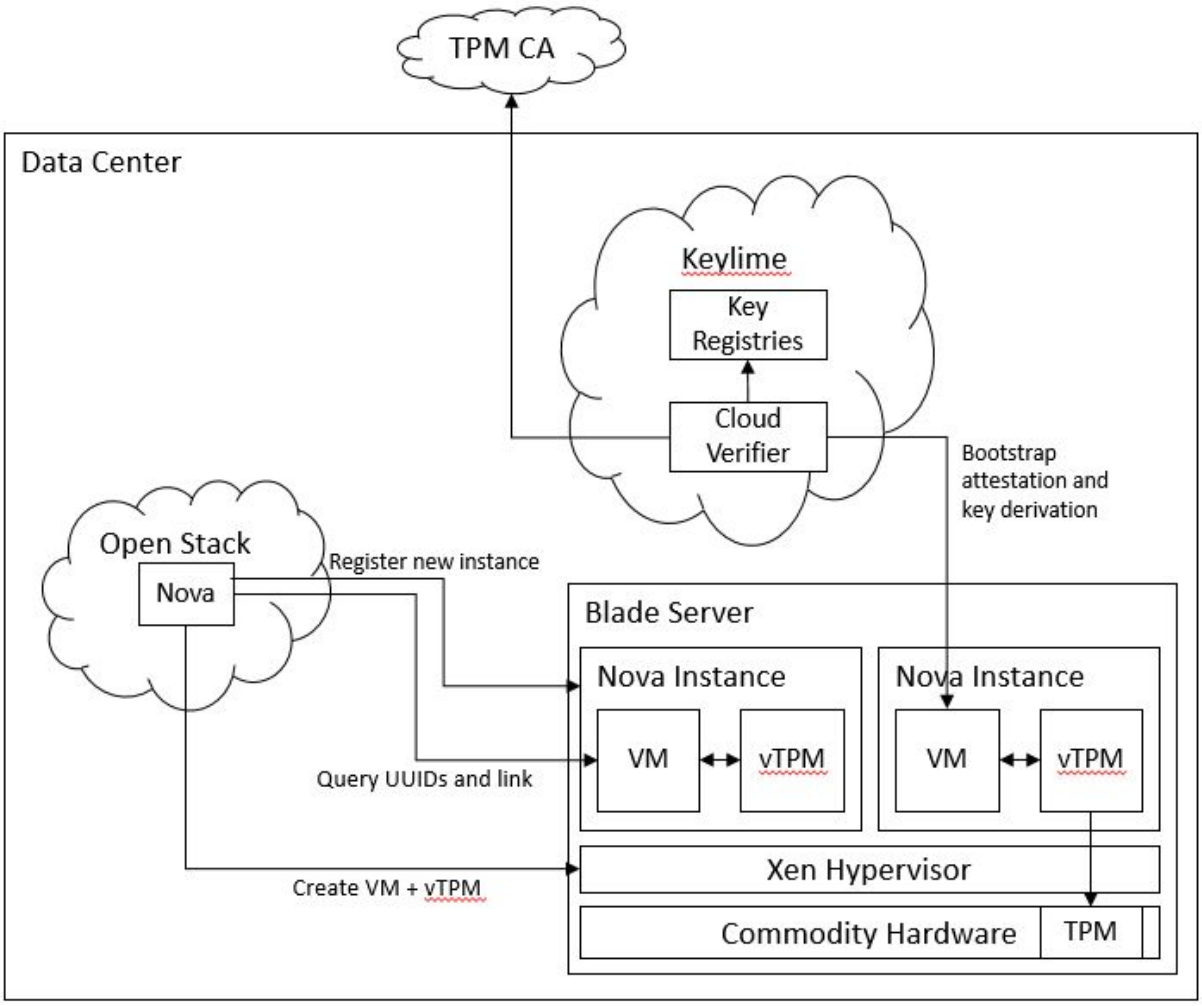
- Do not have to deal with migration
- Do not have to deal with imaging
- Storage of AIKs indexed for each node
- Integrate VM & vTPM setup into OpenStack
- Linking lifecycle of vTPM to VM (startup & shutdown)

3. Solution Concept

We will be building on Lincoln Lab's work on trusted computing on IaaS installations known as keylime. Keylime comprises a set of software components that secures the bootstrap process of spinning up a VM using attestation and implements a secure key derivation protocol to start up higher level security services. Virtual TPMs (vTPM) provided by Xen provide the necessary hardware rooted chain of trust necessary for attestation. The Xen implementation of vTPM places it within its own domain and unikernel which allows it to coexist with other VMs on the hypervisor. Multiple instantiated vTPMs then share the physical TPM using an extra "deep quote" query when the vTPMs need to access the physical TPM.

This project will first build up a development cluster consisting of a Xen and OpenStack installation. Support for Xen's vTPMs will be added to OpenStack by augmenting Nova's life cycle management API for compute instances. Whenever an image is launched, it should also trigger the creation of a vTPM on the hypervisor. The UUIDs of these two new instances must be queried and then stored in a registry for future management operations. Afterwards, the vTPM must be registered to the new compute instance to allow for the secure bootstrap process.

On the OpenStack cluster, we will run the keylime cloud verifier services and necessary registries as part of the data center management layer. With that, a complete end to end solution for trusted computing on OpenStack can be demonstrated.



Design Implications and Discussion

Augmenting OpenStack with Xen's vTPM through Nova's APIs is a natural extension to provide trusted computing services. The linked nature of vTPMs to Nova's VM based compute instances means that their life cycles are also linked. Therefore the creation and destruction of vTPMs follows that of the VMs they are linked with down to the exact server they are created on. Further, since Nova is in charge of VM creation on Xen it should be straightforward enough to extend that interaction with Xen to create the vTPM and linkage.

4. Acceptance criteria

Because we are going to establish a safe and efficient environment which is totally isolated from hardware for vTPM and VM, the first step is to comprehend Xen and find out the method to plant it in our project. For us, the expectation of Xen is that it would host a bunch of virtual machines simultaneously.

What really matters in this project is that we try to build an integrated cloud trusted computing architecture comprising vTPM and VM. This is an innovative part, which means that not many resources exist, so we have to set up and test our vTPM and VM in advance. Some work has been done between TPM and computers, but it is still necessary for us to figure it out based on vTPM and VM. The minimum requirement for this part is that vTPM and VM are connected with each other and manage the ID coming out of vTPM.

Merging above aspects into OpenStack is the final and practical part. Just as Nabil said, getting these into OpenStack is a large, stretching and commercial process. What can be expected is that we achieve our goals - integrating vTPM capability into OpenStack and maintain same lifecycle.

Furthermore, we could earn some bonus if we could finish some of targets below.

1. Utilize OpenStack components like Nova.
2. Get openstack to create extra vTPM domain, and connect domain to instance.
3. Integrate our project with Lincoln Lab’s work.

5. Release Planning:

1. Setup the development environment
    - Take inventory of available hardware resources from Lincoln/University for creating development cloud.
    - Create a working Xen deployment with vTPM support for creating vTPMs and VMs.
    - Download, build, and deploy stable Open Stack source code.
    - Integrate Open Stack deployment with Xen deployment and spin up a VM.
2. Be able to create vTPMs from OpenStack
    - Setup Jenkins server to test and deploy changes to Open Stack source
    - Augment Nova to create vTPMs and link them to the VM
3. Integrate Keylime cloud software
    - Test attestation and bootstrapped key derivation protocol.
    - Perform security audit of implementation
4. Demo the complete stack
    - Debug and troubleshoot any major issues
5. Finalize Project
    - Debug and troubleshoot remaining issues
    - Writeup necessary documentation
    - Source code refactoring
    - Double check that everything still works.