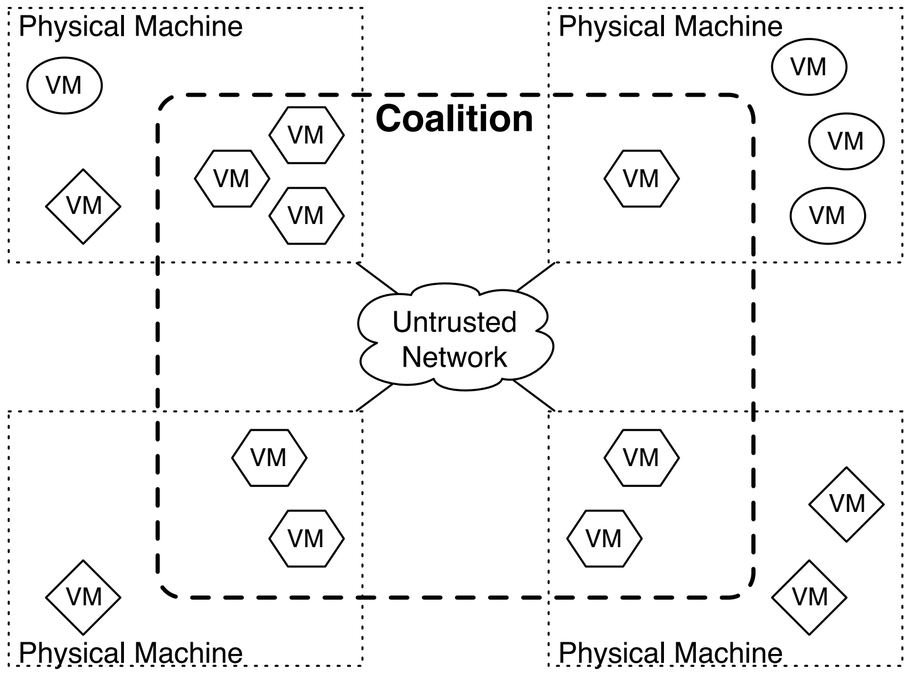
# Shamon: A Shared Reference Monitor for Distributed Mandatory Access Control

Luke St.Clair, Josh Schiffman, Trent Jaeger, Patrick McDaniel

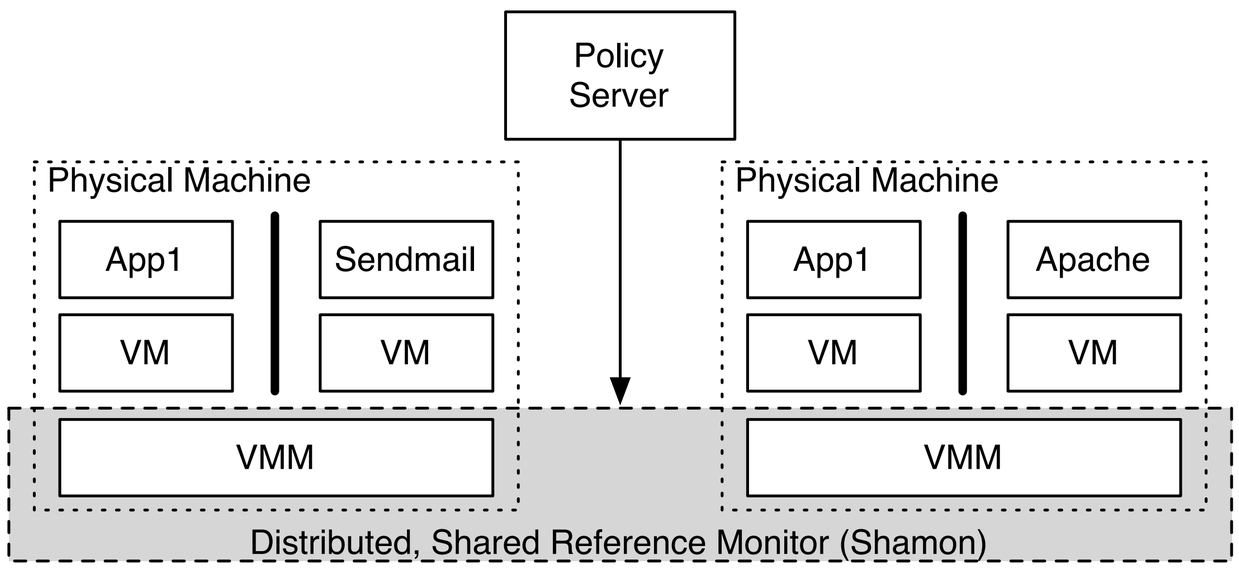
Problem:

We want to develop trust in the enforcement of security goals across many machines on an Internet scale, but fear of malicious administrators, compromised machines, and unwitting leaks of sensitive data make this difficult. Additionally, the complexity of operating systems makes it difficult to say anything meaningful about the security of another system in a traditional setting.

Our goal is to achieve the guarantees of a **reference monitor** (tamperproof, completely mediated, simple enough for verification) in a distributed setting. We would like to establish a **coalition** of virtual machines within which we can make some guarantees about the security of communication and the enforcement of policy. This coalition will be governed by a central authority, called a **Shamon** to enhance scalability and accommodate dynamic changes to the coalition.




## Vision




A Distributed, Trusted, Reference Monitor (DTRM) is established to enforce policies on physical machines and virtual machines. This is the entity that is formed to control the coalitions of VMs.

Virtual machines run on the physical machines to provide applications. This allows us to reason at a much coarser granularity than the operating system level to govern sharing and access control.

Policies then govern the relationships between VMs, forming coalitions. These policies govern which VMs are in which coalitions, which coalitions can talk to each other, and how they may communicate.

Sharing between VMs is governed by sHype, while SELinux governs how data is transfered from one VMM to another. SELinux policies govern this relationship, but they are much less complex than governing sharing between all the subjects and objects on an opertating system.

For this to scale, we must have a way of managing attestations, membership, and trust.

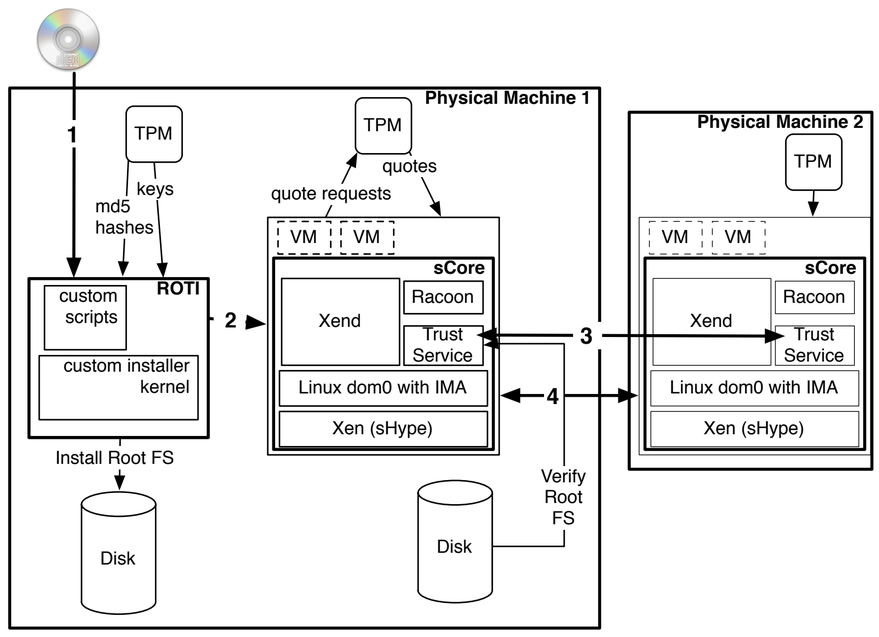
## Future Work

Given that we want to establish a shared reference monitor on an internet scale, we must be able to create, move, monitor, and delete virtual machines in a scalable fashion. To that end, we create different management entities to protect **coalitions** of virtual machines, physical sCore, and distributed applications. This will allow the Shamon system to support complex policies governing access to computing resources, protection of VMs, network communications between VMs and sCore, and membership in application-specific coalitions.

Finally, we will also be reasoning about the properties of the enforcement system. The enforcement policy will have to be distributed or reconciled to each machine in the coalition, and **trust relationships** will have to be established between hypervisors. For instance, we will show that the semantics of the trust logic are correctly enforced in the system policy. We also will consider the **consistency, soundness, and completeness** of the reference monitor in order to evaluate its effectiveness.

## Current Work

Unlike previous approaches, we create a way to establish trust in both data and code. In order to do this, we use a **root of trust installer**, or ROTI. This ROTI contains code with digital signatures capable of installing the necessary core components to form a **secure, distributed reference monitor (sCore)**. In practice, this is a fully automated installation CD, which installs Xen, a dom0 kernel, and a minimal set of utilities, while using the TPM to guarantee the origins of data in the dom0 (published at ACSAC '07). The integrity of data in the sCore is preserved across boot cycles, and is remotely verifiable by remote parties.




Sponsored by IBM Research