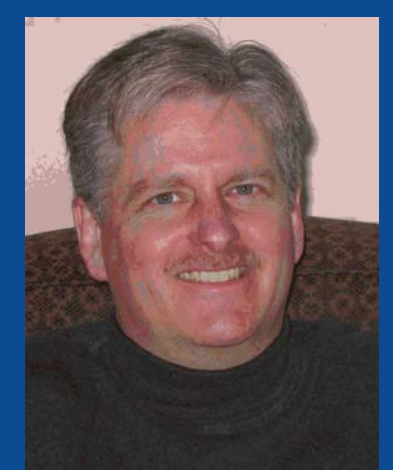


Shamon: Systems Approaches for Constructing Distributed Trust

Trent Jaeger and Patrick McDaniel, Penn State (<http://siis.cse.psu.edu/vm.html>)



Trent Jaeger



Patrick McDaniel

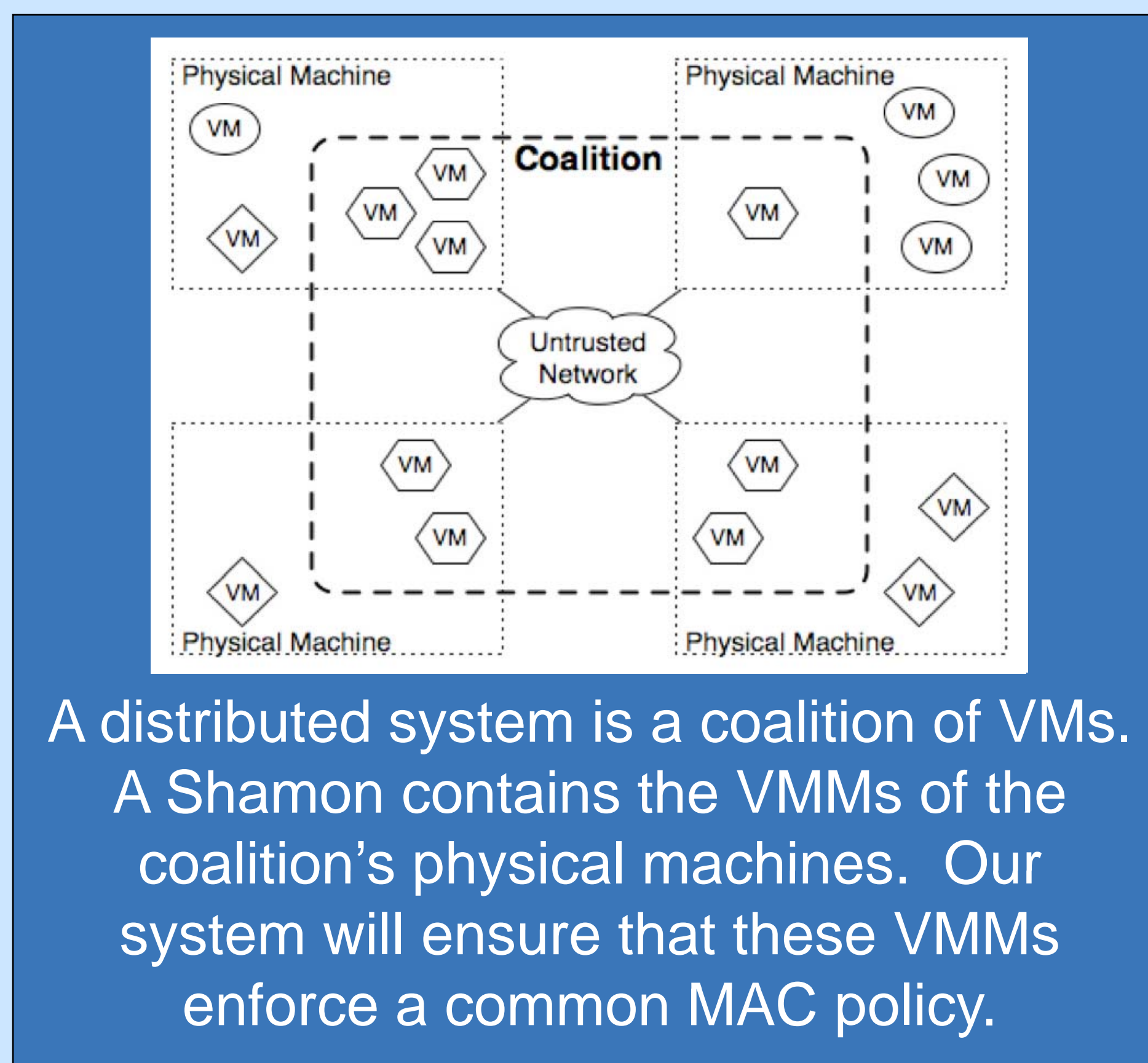
Shamon: Shared Reference Monitor

Recent advances in **virtualization** and **trusted computing hardware** provide an opportunity to construct large-scale, distributed authorization systems that **achieve reference monitor guarantees** (tamperproof, mediation, simplicity) across systems.

This project consists of two main tasks:

- Construct a security infrastructure to **enforce mandatory access control (MAC)** over distributed VM systems
- Develop and maintain **distributed trust** in this infrastructure based on reference monitor guarantees

Enable the development of large-scale, distributed systems, such as a university-wide virtual classroom, that can enforce MAC guarantees



Approach and Impact

New approach

- Define reference monitor guarantees for a distributed system
- Construct a trusted computing base for which those guarantees can be proven
- Develop a logic for distributed trust in reference monitoring

Research Impact

- Enforce coherent MAC policy in distributed systems
- Define an approach for building integrity-verifiable reference monitors
- Enable management of distributed trust at runtime

Trust in the integrity of distributed MAC enforcement is defined by its individual reference monitoring components. We have defined the properties for such components, manifested in our **Shamon Core (sCore)**

The trust in an sCore is derived from verification that it derives from a trusted installer, the **Root of Trust Installation (ROTI)**

The ROTI configures the sCore component, and uses TPM Sealing to map the ROTI to its sCore files, the **sCore-ROTI Binding (SCRB)**

When an sCore is run, it can prove its ROTI origin to remote party using a TPM Attestation comprising its few sCore programs and the sCore-ROTI Binding (SCRB)

