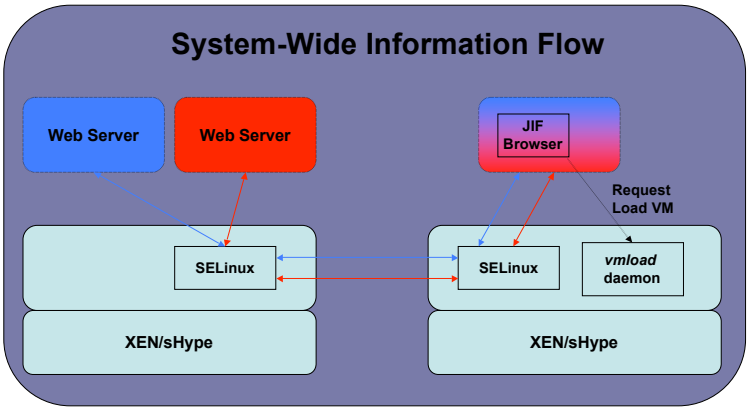
Virtual Machine based Network Access Control

Yogesh Sreenivasan, Sandra Rueda, Trent Jaeger and Patrick McDaniel

We propose enforcement of *information flow policies* in a distributed environment, unified across the virtual machine, operating system and application layers.

- Information flow policies have traditionally been dealt within the realm of Operating Systems.
- Recent advances in *Security typed languages* such as JIF, ensure enforcement of information flow policies within applications.
- We intend to extend the information flow guarantees provided by the application, in a verifiable way, to a distributed virtual machine environment leveraging the *MAC enforcement* provided by the VMM and the *Labeled IPsec* mechanism.



Information Flow Enforcement

Information flow policies are enforced independently at different layers of the system. To have an effective enforcement, we propose integration of all the layers. The JIF Browser and SELinux OS provide Information Flow guarantees at the application and Operating System Level. We are extending the *guarantees at the virtual machine and network layers*. The Virtual Machines are run on a secure VMM which acts as a secure platform on which all computation takes place.

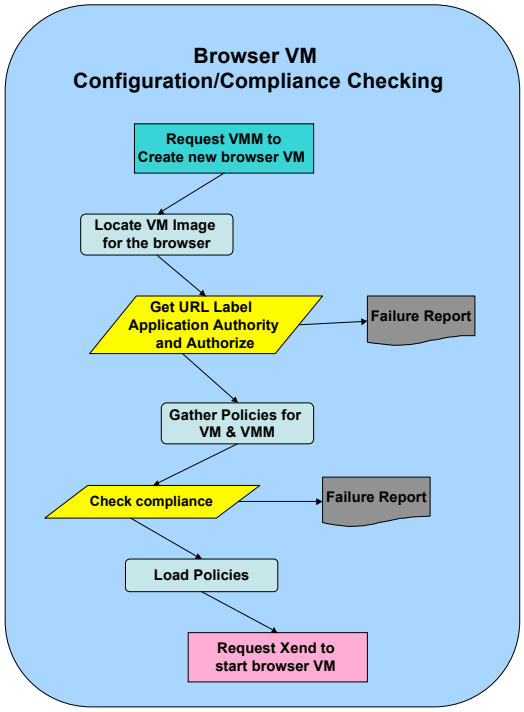
Our protocol for system wide regulation of information flow has two phases.

Configure/Check Compliance of new Browser VMs.

- Gather and update the JIF, SELinux and Labeled IPsec policies for the new browser VM.
- Gather and update SELinux, Labeled IPsec and sHype policies for the secure VMM.
- *Check for compliance* of Browser VM with VMM flows and also between SELinux and JIF Policies.

Enforcing the Information flow.

- Establish a Labeled IPsec tunnel between the browser VM and VMM. *Labeled IPsec mechanism* allows association of SELinux labels to IPsec tunnels.
- The secure VMM should authorize all the network packets based on its security label.
- Extend the IPsec tunnel segments to the destination VMM to correctly convey the labels.



Future Work

We envision extending the infrastructure to support enterprise level web applications. We plan to extend the information flow guarantees across different components of the application like Database Servers, Content caches etc.

We also intend to extend the information flow policies to support and enforce integrity levels at a finer granularity.

Publications

Trent Jaeger, Rainer Sailer and Yogesh Sreenivasan. **Managing the Risk of Covert Information Flows in Virtual Machine Systems**. ACM Symposium on Access Control Models and Technologies (SACMAT). June 2007.

Work Sponsored by DTO, NSF