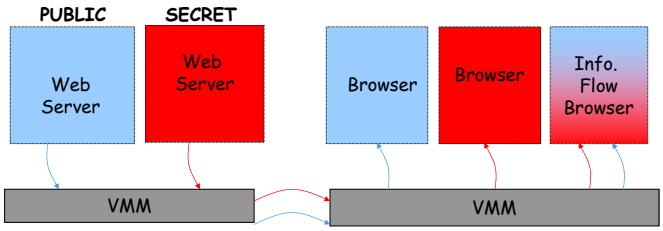
System-wide Information Flow Enforcement

Guruprasad Jakka, Dave King, Sandra Rueda, Yogesh Sreenivasan
Trent Jaeger, Patrick McDaniel

Information flow enforcement, which was historically focused in operating systems, can be unified across the virtual machine, operating system, and application layers to achieve more effective and more flexible enforcement than the operating system alone

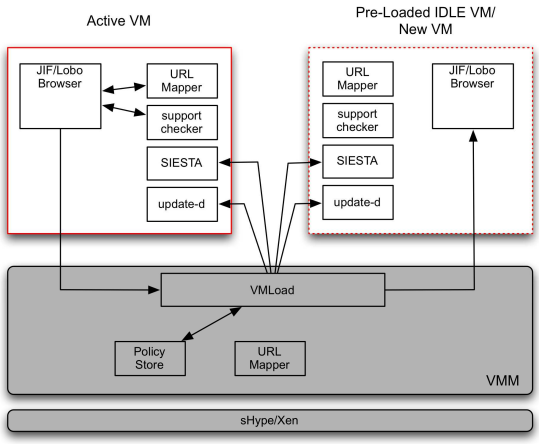


Framework

- Develop the info flow-aware FlowwolF browser client that enforces system security goals
- Enable SELinux systems to verify FlowwolF's compliance with OS goals
- Extend these info flow guarantees to the virtual machine and network

The FlowwolF Browser System enforces a system policy over browsing

If a URL is requested that is not authorized for that Browser VM, then the FlowwolF Browser System will automatically generate a new VM



Improving IF Control by Integrating Enforcement Layers

From Independent Enforcement

- Untrusted, black-box applications
- OS cannot be sure that applications enforce system security goals
- Incompatible enforcement mechanisms across layers

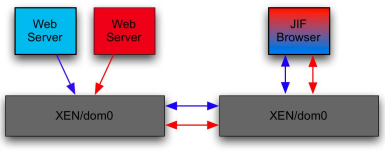
To Integrated Enforcement at all Layers

- Information flow-aware browser
- OS verifies and leverages application enforcement of system security goals
- Common security goal across system layers: OS, VM, network

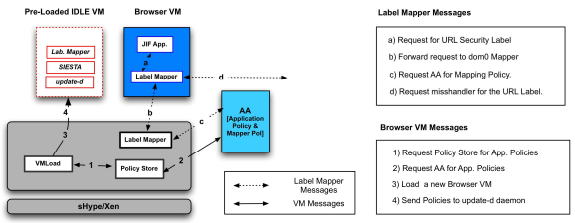
Traditionally, information flow requirements are enforced independently at separate layers of the system. *We claim that effective and flexible enforcement requires integration of enforcement at all layers*:

- *Security-typed languages* (STLs) provide information flow guarantees at the application layer for a browser client;
- *Compliance* of FlowwolF (STL browser) with system security goals must be verified before execution – FlowwolF policies are automatically compose with system policies;
- *Security mechanisms* at each layer (application, system, virtual machine and network) must be able to leverage information flow labels to enforce coherent policies

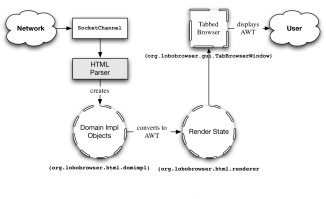
FlowwolF can access read and blue web servers from one process safely



FlowwolF bootstraps new Browser VMs when necessary to acces a web page



FlowwolF is architected to control Information flows among its objects



(Dashed classes need to be Jif-ified)

Publications

Sandra Rueda, Yogesh Sreenivasan, Trent Jaeger. **Flexible Security Configuration for Virtual Machines.** Computer Security and Architecture Workshop (CSAW) 2008.

B. Hicks, S. Rueda, T. Jaeger, P. McDaniel. **From Trusted to Secure: Building and Executing Applications that Enforce System Security**. USENIX Annual Technical Conference, 2007.

Sponsored by AFRL and IARPA