Goals are ambiguous
Administrators configure policies, not goals
Classical information flow goals are too restrictive
We need to relate policies to goals
Complete manual specification is impractical

VM-Systems

VM-systems have a single VMM policy and several OS and network MAC policies.
A VM-system is compliant with an information flow security goal, if all the flows enabled by the policies are authorized by the goal.

Compliance

Challenges

Goals are ambiguous
Administrators configure policies, not goals
Classical information flow goals are too restrictive
We need to relate policies to goals
Complete manual specification is impractical
VM-Systems are complex
They involve multiple policies (VMM, OS, network)
Composing all policies into a single graph would prevent effective analysis

Approach

Problem: how to automatically deduce goals and map policy labels to goal labels.

Use the VM-system configuration to obtain security goals. There is domain knowledge in the VM configuration that we can use to deduce default conservative goals. We also enable administrators to make refinements.

Use top-down view of the system to evaluate information flow compliance. We do not need to integrate all the policies into a single information flow graph. Instead, we use inter-VM flows first to assess information flows before we assess flows within VMs.

Analyze internal information flows if conflicts arise at the higher level view. We also define a comprehensive set of possible resolutions.

We use system domain knowledge and an iterative refinement to deduce goals, to automatically map policy labels to policy goals, and to evaluate compliance.

A system configuration defines domain information that implies security requirements. For instance: if a VM domU depends on a VM dom0 then dom0's integrity must be higher than domU's integrity.

Analysis Tool

We developed an Eclipse plug-in to define VM-systems, load their policies, evaluate compliance, display results, and suggest options to resolve conflicts. The purpose of the tool is to assess administrators in the configuration of a secure system.

Publications