Breaking Down the Walls of Mutual Distrust

B. Hicks, S. Rueda, T. Jaeger, P. McDaniel

We want to protect the secrecy of confidential data

We have OS information flow controls, but many applications are entrusted with data of multiple secrecy levels

Language extensions enable applications to *provably* enforce information flow requirements, but the OS is ignorant of their existence

→ Information Flow Security

→ OS Information Flow Controls are Inadequate

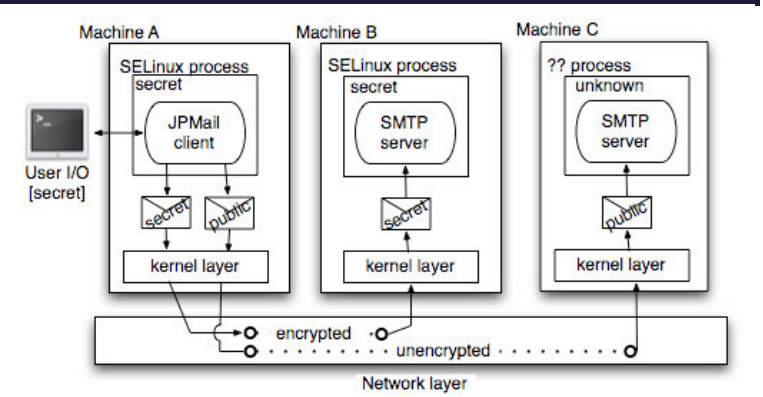
→ Comprehensive Information Flow Enforcement Using OS and Application Controls

End-to-End Information Flow Enforcer

We are evaluating feasibility, design, cost and performance of an infrastructure for supporting end-to-end information flow policies by integrating them at three different layers: application, operating system and network.

We use JIF for supporting Information Flow policies at the application layer, SELinux for supporting policies at the OS layer and Labeled IPsec for supporting policies at the network layer.

The enforcer enables the cooperation of application, OS and network to preserve secrecy requirements by provable information flow control.



JIF

JIF: Java Information Flow

JIF allows a programmer to incorporate Information Flow Policy Enforcement into an application.

JIF is a Java extension developed to implement an Information Flow model. Data are augmented with labels that define Information Flow Policies.

Information flows between locations with different labels only if that information flow does not lose policy restrictions (information is not being leaked).

SELinux

SELinux: Security-Enhanced Linux

SELinux uses Mandatory Access Control to enforce Information Flow Policies in the OS.

The architecture requires to define a label most known as security context for every element in the system.

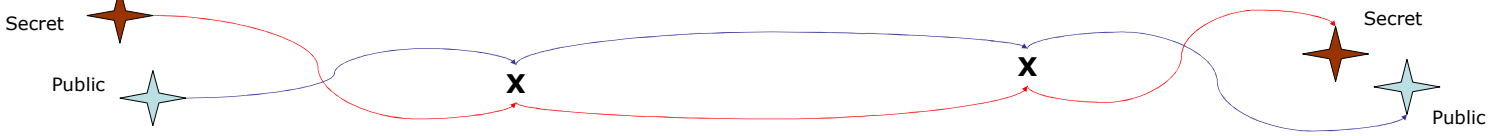
Information flows between locations with different security contexts (labels) only if the MAC allows it, based on predefined rules.

Labeled IPsec

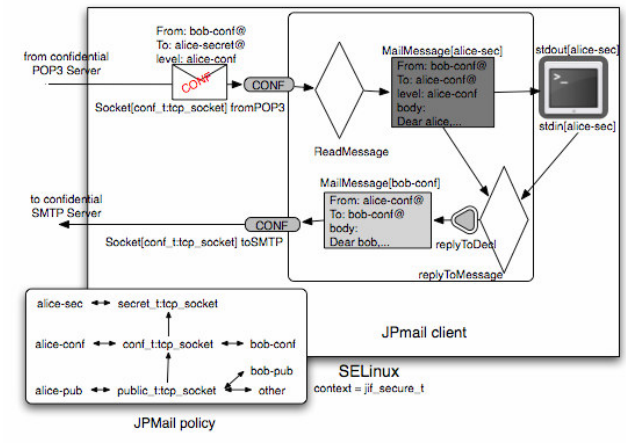
Labeled IPsec extends Mandatory Access Control to the network.

Extension to the IP network layer developed for supporting authentication, integrity and confidentiality.

Information flows (network communication is established) between two machines only if the MAC mechanism allows it based on predefined rules.



JPMail on Enforcer



Handling of various levels of flows + Declassification

Results and Future Work

Findings:

Feasibility: We have the tools to build the end-to-end Information Flow Enforcement Infrastructure.

Design: It is possible to manage multiple security levels within a single execution of an application. Cross layer Policy compliance was informally defined.

Cost: Application code was simplified by moving some operations to the OS and network.

Performance: Additional overhead is not significant.

Enforcer Advantages:

Granularity and Efficiency: the appropriate system has more information to make secure decisions.

Simplification: program code is reduced and becomes independent of security functions such as encryption.

Future Work:

-More JIF Applications.

-Information Flow Guarantees at OS level.

-Integrity Information Flow.

-Test-bed for more precise performance evaluation.

Sponsored by IBM Research