cation

ations are mediated

nsistently applied

R

 Policy Design and Analysis
 Goal-based policy design; Information flow-based policy analysis
 System Attestation
Hardware-based Integrity measurement; Information flow measurement
Appl

ating Sys
sor

H
a
r
d
w
a
r
e

essing via known filters

Define Security Goal
Protect Integrity of Application
Enforce Security Policy In Linux UserVM via LSM and SELinux policy
In Xen via isolation and coalition policy
U
s
e
r V

U
s
e
r V

sshd_priv

Unexpected low integrity flows:
- Modified executables
- Modified inputs