



# Finding Attack Surfaces in Programs PENNSTATE System Wide



Sandra Rueda, Divya Muthukumaran, Nirupama Talele, Hayawardh Vijayakumar and Trent Jaeger

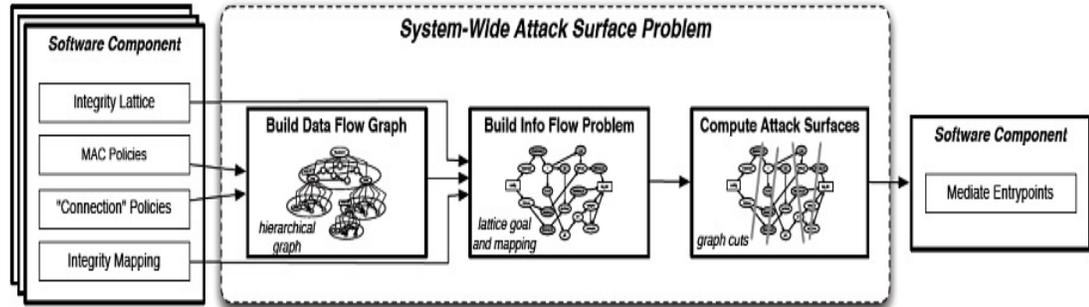
## Problem

- Most distributed systems are composed of several components with their individual policies interacting with each other. This increases the complexity of identifying how threats may propagate in the system.
- The methods to overcome these are largely reactive rather than proactively finding the entry points accessible to the adversary and defending them.

## Key Observation

- Off-the-shelf components often have mandatory access control policies and "connection policies", such as firewall policies, that describe how they interact with each other, enabling automated computation of a system-wide data flow graph.
- Application-level information flow requirements can then be evaluated over such data flow graphs to find accessible entry points automatically.

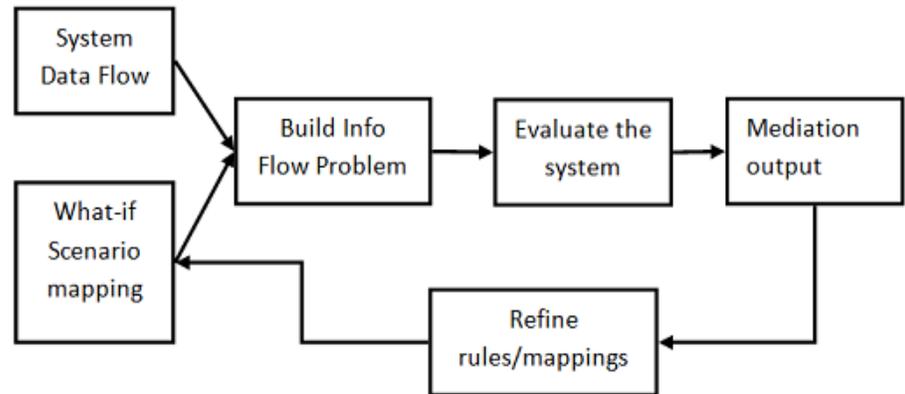
## Solution



## Building Information Flow Problem

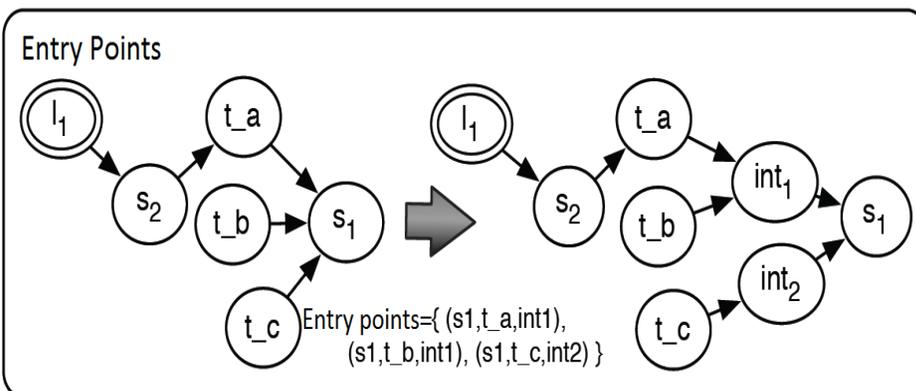
### "What-if scenario analysis":

- The security level mapping to the types in a policy are not currently determined by any formal constraints and are largely assigned based on expert knowledge. The security requirements met by the type might not confirm with the security level assigned and the analysis might lead to certain false negatives.
- We use a what if scenario analysis method by assigning one level lower integrity level to the types based on the program integrity wall to identify :
  - Additional mediations needed if any
  - Determine that system cannot be mediated and will enforce the security constraint on type.



## Computing Attack Surfaces

### "Entry Point Analysis"



## Results

### Part 1:

Total entry points	Mediated entry points	Mediation effort reduction
1815	107*	94.1%

The results show that out of all the runtime entry points for programs in the system only a few require mediation. Thus finding minimum cost mediations to solve all information flow errors in the system.

\*The total mediators found are 528 out of which only 107 unique, the mediated entry points are repeated in different VMs which does not add extra cost.