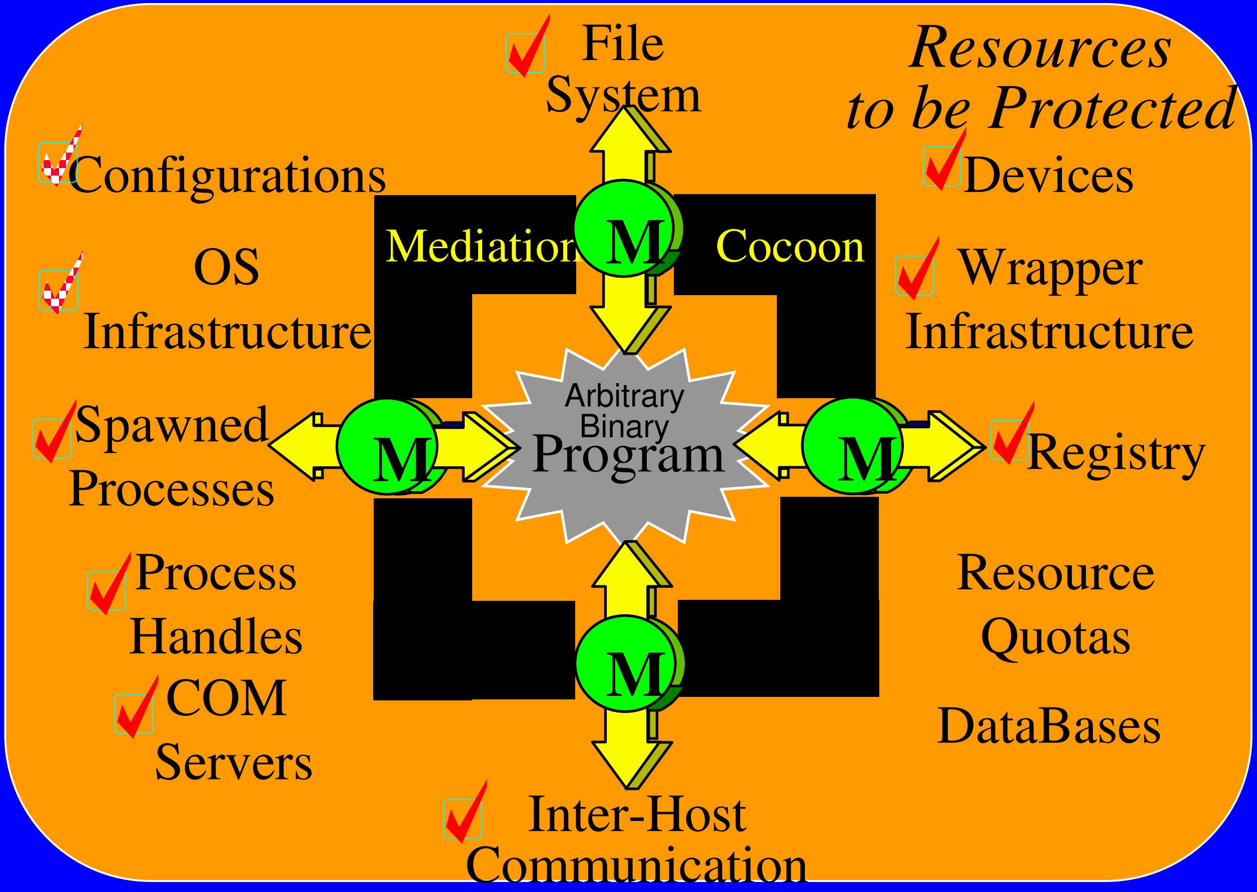
TEKNOWLEDGE

• Name of Organization:	Teknowledge
• Lead Investigator:	Bob Balzer
• Current Team Members:	Neil Goldman Dave Wile

TEKNOWLEDGE

Contained Execution



- Implements assignment of privileges to applications
- Already applied to many popular COTS products (policies built)
- Maturity – in use on daily basis
- Non-ByPassable and Hardened against attacks on itself
  - Gave Red-Team Administrator privileges & execution of their own code
- *Contained Execution* – Process-Level Virtual Machine

TEKNOWLEDGE

Contained ~~Wrapped~~ Execution

- Goal: Safely Execute possibly Malicious Code
- Approach:
  - Mediate potentially harmful operations
  - Apply Authorization function (Allow, Contain, Deny, Abort)

    Unaltered

    Safe
  - Contained operations only affect wrapped process
- Problems
  - Configuration ~~difficult~~ easy

    Allow desired changes

    Contain everything else
    - Tight policy generates many false positives
    - Loose policy leaves room for undetected malicious activity
  - ~~Early~~ Late authorization decision ~~required~~ allowed (after execution)

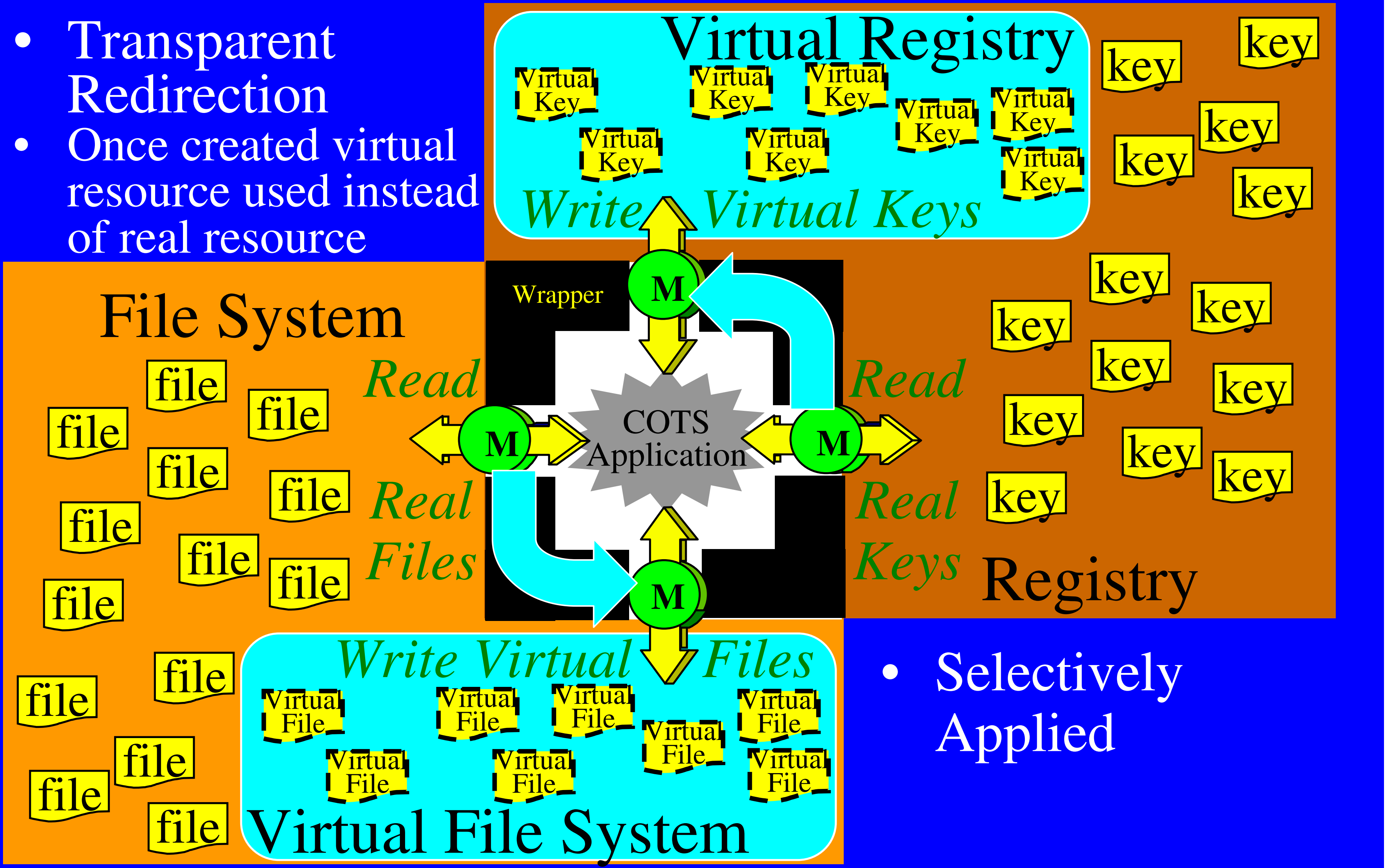
Desired Changes

Attachments	=>	None
Editors	=>	Edited document

TEKNOWLEDGE

Virtual Resources contain effects within process itself

- Transparent Redirection
- Once created virtual resource used instead of real resource



- Selectively Applied

TEKNOWLEDGE

Contact Information

Name:	Bob Balzer
Title:	Chief Technical Officer
Organization:	Teknowledge
Email address:	balzer@teknowledge.com
Phone number:	(505) 982-1793