

# SELinux Thoughts/Direction

Trent Jaeger, IBM Research

[jaegert@us.ibm.com](mailto:jaegert@us.ibm.com)

Doc Shankar, IBM Linux Technology Center

[dshankar@us.ibm.com](mailto:dshankar@us.ibm.com)

# MAC vs. DAC

- Discretionary Access Controls (DAC)
  - Traditional protection mechanism: ACLs, permission bits, etc.
  - Controlled by individual user or application program
  - Vulnerable to Trojan horse and virus attacks
- Mandatory Access Controls (MAC)
  - Developed originally for defense applications
  - Policy mandated by enterprise, rather than user
  - Kinds of MAC protection
    - Bell and LaPadula Secrecy Model to prevent leakage of information to unauthorized recipients
    - Biba Integrity Model to prevent unauthorized tampering or sabotage
    - Role-based Access Control enables enterprise control of user-role and permission-role mappings
    - Type Enforcement flexibly defines access from subject types to object types
    - Domain and Type Enforcement enables transitions between subjects

# LSM and SELinux MAC

- Linux Security Modules (LSM) hooks accepted in Linux 2.6
  - Excepting skbuff networking hooks
- Around 200 hooks
  - About 150 are for access mediation
  - Others for allocation/free, labeling, ad hoc management
- SELinux module performs authorizations behind these hooks (example LSM)
  - Most comprehensive, mature, and detailed LSM
  - Supports multiple policy models
- SELinux module included in Linux 2.6
  - Example Domain and Type Enforcement policy under development by SELinux community

# SELinux Deployment

- Linux Security Modules Framework
  - Low-level network hooks to label incoming packets
  - 2.6 does not include these (10?)
- Kernel Integration
  - Integrate SELinux with IPSec
  - MAC labeling on IPSec flow
- Application Level Authorization
  - XWindows
  - Hooks to enforce SELinux policies within X
- Policy Issues
  - Sys Admin. decomposition
  - Sys. Admin. has too many privileges (need to limit)
- Policy Management
  - Ensure policy achieves security goals

# Security Verification

- Source Code Security Analysis
  - Static Analysis
    - Verify all controlled operations are mediated by at least one security check
    - Tool - CQUAL
  - Dynamic (runtime) Analysis
    - Verify all controlled operations are authorized
    - Tool – Vali
    - Complete Mediation – Do all security-sensitive operations follow an authorization hook?
    - Static Tool consulting
    - LSM Bugs found, tool has been open sourced
    - Is it possible to use this for assurance?
- Access Control Policy Analysis
  - Verify that policy enforces integrity requirements
  - Tool – Gokyo
  - Identifies Biba Integrity Violations
  - Analyzed SELinux Policy for Apache Administration – found 17 conflicts in 2.4.16
  - Find SELinux’s minimal TCB
  - Is it possible to use this for TCG type analysis?
- Linux Analysis Tools Project Reference - [www.research.ibm.com/vali/](http://www.research.ibm.com/vali/)

# Future Work

- Certification
  - MAC profile – LSPP, MRMLOSPP?
- Productize
  - Integrate security function
  - Robustness/Hardening
- Policy Management
  - Full tool suite to customize SELinux example policy to meet goals
- Distributed SELinux
- Deployment (Apache, DB2, Websphere,..)
- Pilot Application Projects