



Adding Strong Access Controls to Linux

September 26, 2000

Grant M. Wagner
National Security Agency
gmw@tycho.ncsc.mil

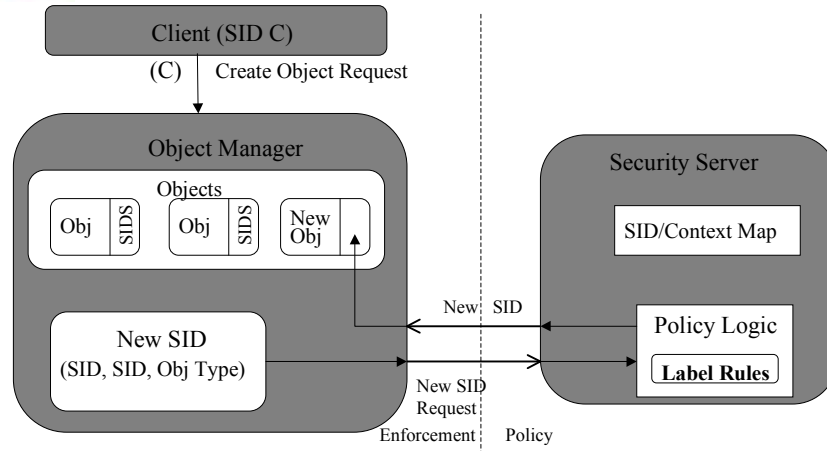


Basic Design Principles

- Flexible policy and mechanism
- Separate policy from enforcement
- Abstract policy relevant data
- Limit performance impact
- Linux remains Linux



Basic Architecture



Example Types of Policies

- Separation Policies
- Containment Policies
- Integrity Policies
- Invocation Policies



Policy Primitives Supported

- Identity
- Roles
- Domains & types
- MLS labels



Linux Controls

- Process mgt. (fork, exec, /proc)
- File system (file systems, files, directories, file descriptions)
- Device mgt. (/dev, ioctl)
- IPC
- Networking
- Capabilities



Other Efforts

- Hardening efforts
- New mechanisms



References

- www.cs.utah.edu/flux/fluke/html/flask.html
- www.sctc.com/randt/HTML/dtos.html
- www.sctc.com/randt/HTML/final-docs/genpol.pdf