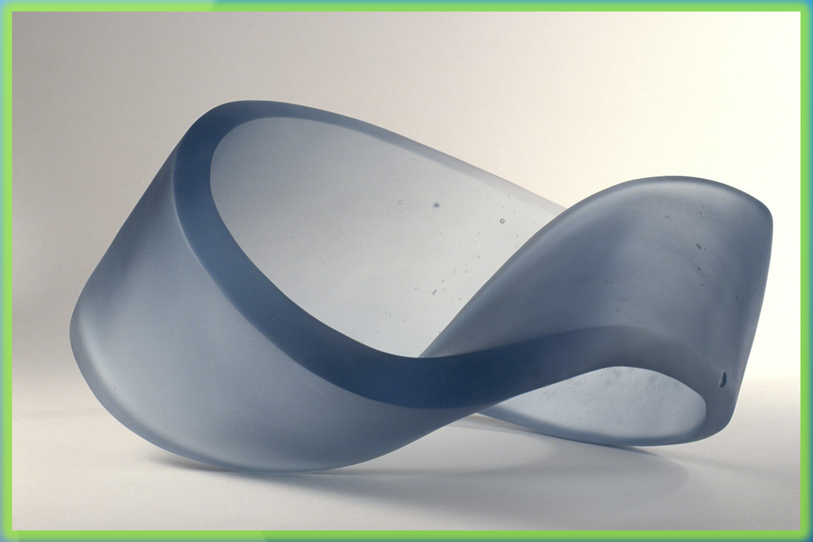
Additional Requirements for MLS



M. Farias,
C. Whitehead
Sabre Systems

Turnkey MLS

- Turnkey ecosystem is ***required*** for adoption and critical mass
- MLS must support REAL workflows / pipelines
- What does this mean?
  - MLS capable services for every (initially most) common enterprise applications
  - SSO/LDAP, RDBMS, Web Servers, Java EE containers, CMS, Version Control, WAN transport, non-relational stores
  - IB/RDMA support for distributed memory systems

SELinux “gap”

SELinux cannot check access to data objects managed by user space applications.

Worth saying twice:

SELinux cannot check access to data objects managed by user space applications.

Progress to Date

- Currently MLS-capable:
  - Apache
  - Postgres
  - Batch Scheduler (PBS PRO)
  - Direct Attached RAID (xfs, ICD-503 certified)
  - SVN
  - Log reduction (Splunk)
- In work / planned
  - SSO via Red Hat IdM (Sabre, LMCO, Red Hat)
  - Authentication Management (Semper Fortis, Seagate, Instrumental)
  - Support for SELinux aware RDMA over IB (Mellanox)
  - WAN Transport via IB/RDMA (Bay Microsystems)
  - AWS Demonstration Environment (Sabre, LMCO)
  - Accumulo (LMCO)
  - Web Container (Tomcat / Jboss EAP)

Apache via mod_selinux

- https://code.google.com/p/sepgsql/wiki/Apache_SELinux_plus

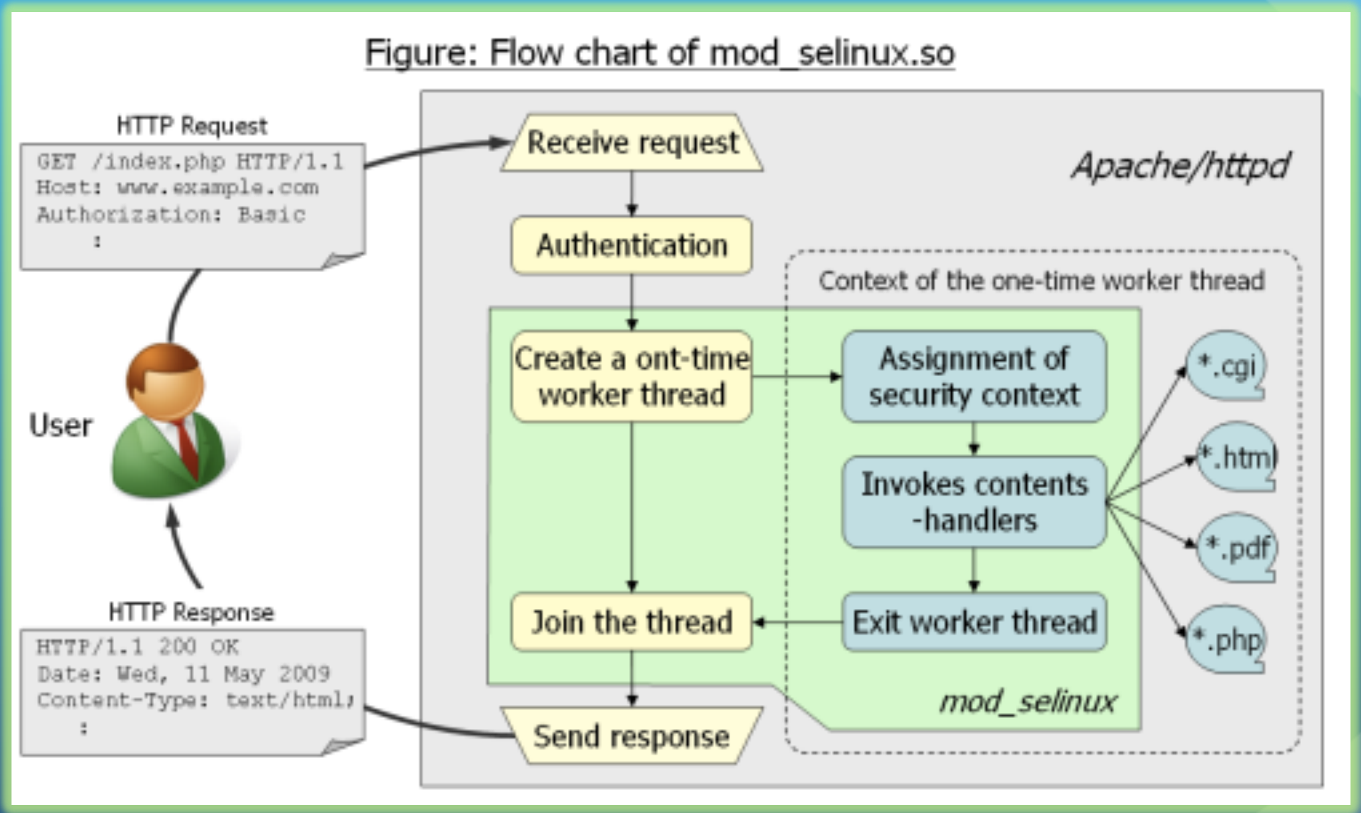


Figure: Flow chart of mod_selinux.so

HTTP Request

```
GET /index.php HTTP/1.1
Host: www.example.com
Authorization: Basic
    :
```

HTTP Response

```
HTTP/1.1 200 OK
Date: Wed, 11 May 2009
Content-Type: text/html;
    :
```

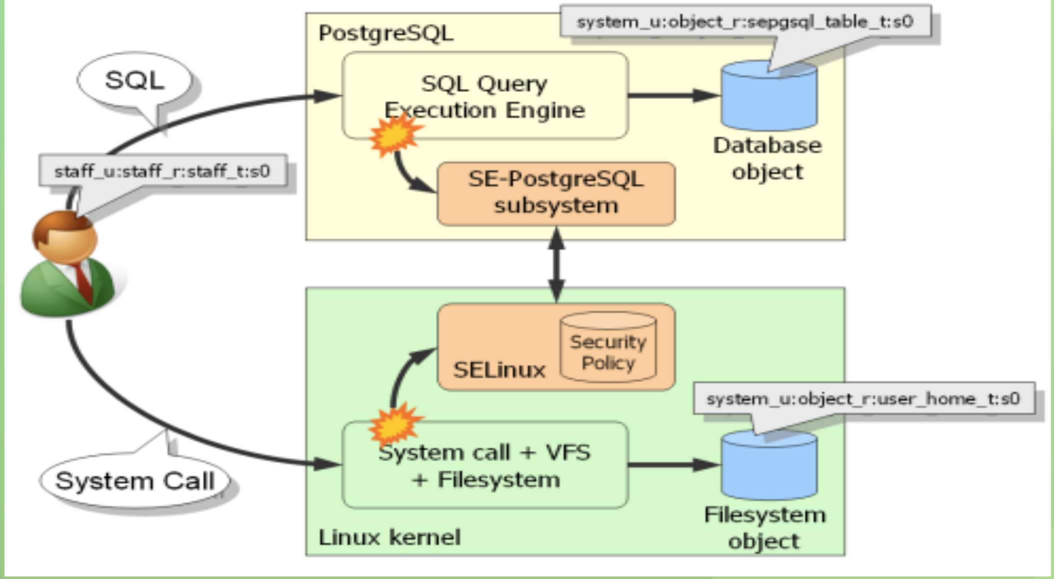
User
Apache/httpd
Receive request
Authentication
Context of the one-time worker thread
Create a ont-time worker thread
Assignment of security context
Invokes contents -handlers
*.cgi
*.html
*.pdf
*.php
Join the thread
Exit worker thread
mod_selinux
Send response

SE-PostgreSQL

https://wiki.postgresql.org/wiki/SEPostgreSQL_SELinux_Overview

- Starting with version 9.1, limited MAC support via sepgsql
- Partnered with Crunchy Data for cell-level as of 9.4

Figure: Concept of SE-PostgreSQL


PostgreSQL
system_u:object_r:sepgsql_table_t:s0
SQL
SQL Query Execution Engine
Database object
staff_u:staff_r:staff_t:s0
SE-PostgreSQL subsystem
SELinux
Security Policy
system_u:object_r:user_home_t:s0
System Call
System call + VFS + Filesystem
Filesystem object
Linux kernel

Batch Scheduler (Altair PBS Pro)

- Through CSCF collaboration with Altair PBS branch exists that is label-aware
- Historically a branch but will merge into trunk on next release

SSO (In progress)

- Plan to leverage Red Hat IdM for single sign on
- PKI-centric

Authentication Management (in progress)

- Site security manager or corporate security officers must centrally manage what individuals (identities) can authenticate-to.
- Authentication profile constantly in flux at enterprise-level, new-hires, personnel assigned, re-assigned to sensitive projects
- Needs to be centralized and roles required to be physically separate. Authentication Manager is not System Administrator.
- MLS-aware back-end (Postgres).
- Ideally build using Apache/Tomcat or Apache/JBoss EAP stack

IB / RDMA

- Working with Mellanox Federal to identify right place in IB specification to inject label information
- Testing to be performed by Cray

AWS MLS Environment

- Goal is to host MLS HPC environment within AWS by the end of the CY
  - Amazon clear innovator; deserve business + yield flexibility
  - Will allow for greater awareness of technology maturity
  - Associated with OpenMLS Consortium
  - Still working out details of hosting organization
  - Low level testing in progress using CSCF RHEL6 RPMs

Requesting Feedback

- Any services we missed?
- Questions?
- Thank You!