Understanding Hardening tools: **SELinux**

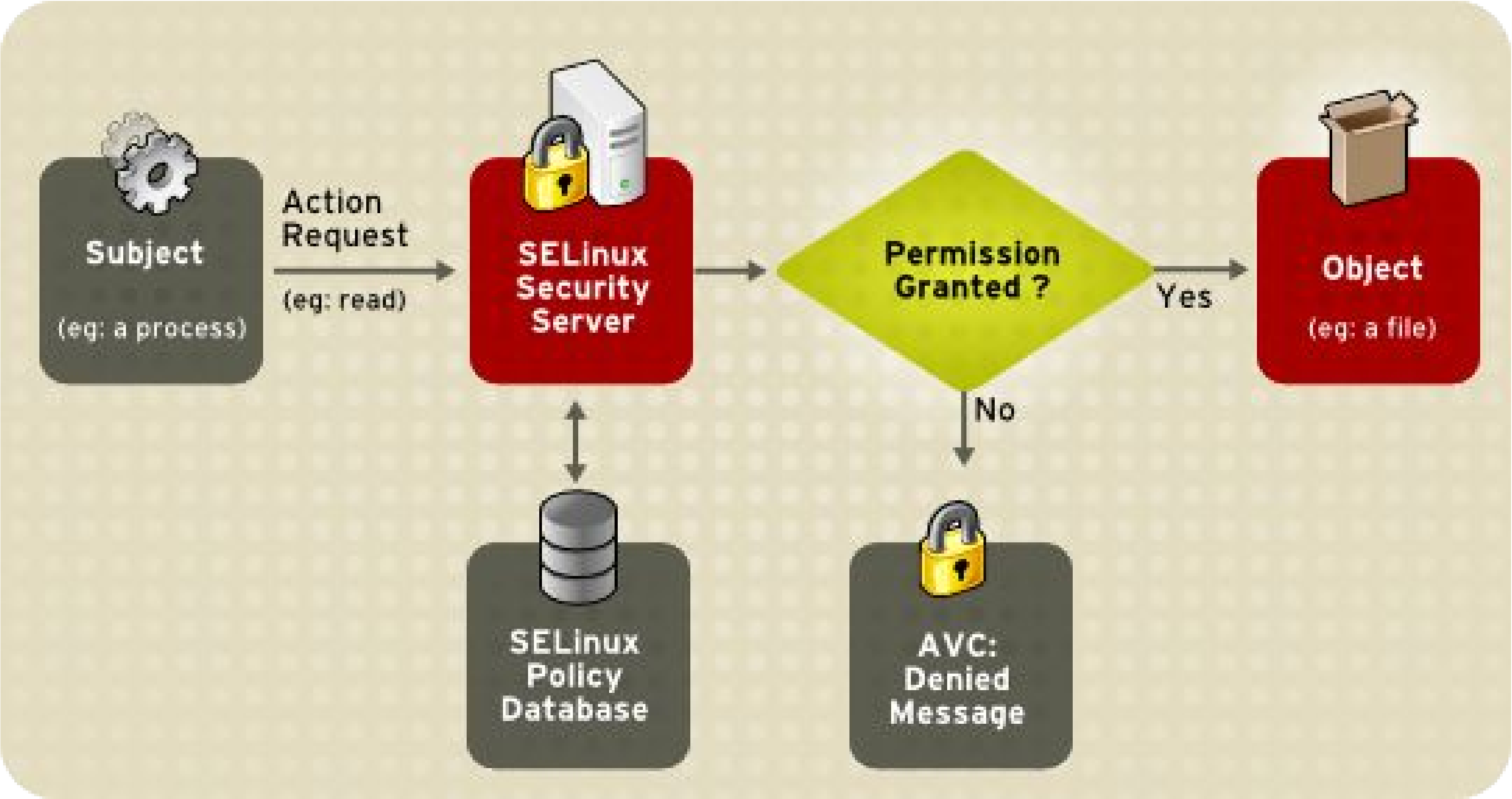
- Development
- Implementation
- Management
- Overall conclusions

SELinux: **Development**

- Started as an implementation of **FLASK OS** security architecture
- Developed by **NSA** and the **SELinux community**
- SELinux and **LSM**, which came first?
- Fully integrated into the 2.6.x Linux kernel

SELinux: **Implementation**

- Label-based security: *user_u;role_r;type_t* , **MCS** - **MLS** and **Type Enforcement**
- Security contexts stored in **ext3 xattr** space: brief history of implementation
- **Targeted | Strict** default policy, Red Hat team
- **LSM** Hooks, **Access Vector Cache (AVC)**


Subject
(eg: a process)
Action Request
(eg: read)
SELinux Security Server
Permission Granted ?
Yes
Object
(eg: a file)
No
SELinux Policy Database
AVC: Denied Message

SELinux: **Management**

- **Installation**->selinux-basics, policy-default and activate
- Switch **-Z** adds SELinux support for commands like **ls, ps**
- **semanage** tool to customize and control SELinux security contexts
- **semodule, sesearch** to show, enable/disable policy modules

SELinux: **Management**

- SELinux uses **audit** daemon to log accesses
- **Permissive** mode just logs denials, useful for debugging
- **audit2allow** command uses log to generate new policies
- Tweak policies on the fly with **booleans**

SELinux: **Overall Conclusions**

- Rather complex default policy…good or bad?
- Once resolved all side-effects conflicts, it provides good security in a short time
- Logging gives us all info we need, audit2allow works just nicely…
- …still we feel no sense of **real control**

SELinux: **Resources**

- SELinux Project (https://selinuxproject.org/page/Main_Page)
- Fedora Wiki (https://fedoraproject.org/wiki/SELinux)
- CentOS Wiki (https://wiki.centos.org/HowTos/SELinux)
- IRC channel (irc.freenode.org channel #selinux)
- NSA FAQ (https://www.nsa.gov/search/?q=SELinux)
- Mailing List (selinux@lists.fedoraproject.org)
- Dan Walsh’s Blog (http://danwalsh.livejournal.com/)