Why Linux is more secure than other operating systems?

Tushar B. Kute,
http://tusharkute.com

Linux and Security

- Linux is an open source operating system, where entire code can be read by everyone but still It is considered as more secure compared to other operating systems.
- As there are more devices based on Linux, it is growing rapidly in the tech market.
- Due to this, more people trust Linux platform.
- To know why Linux has superior internet security capabilities, let us check out some of its security features:

IPtables

- IPtables is a firewall, which is installed on most of the Linux distributions.
- You can implement a greater level of security for your Linux machine with the help of the enhanced features of the IPtables.
- It is used to inspect, set up and manage the tables of IP packet filter rules in the Linux kernel.
- Here various kinds of tables may be defined and each table consists of a built in chains and may also consist of user defined chains.
- Each chain is a set of rules which can match a group of packets. Each rule defines what to do with a packet that matches.
- This is known as a ‘target’, which may be a start to a user-defined chain in the same table.

IPtables

```
rashmi@rashmi-dell:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 104 packets, 15676 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 133 packets, 21374 bytes)
 pkts bytes target     prot opt in     out     source               destination
rashmi@rashmi-dell:~$
```

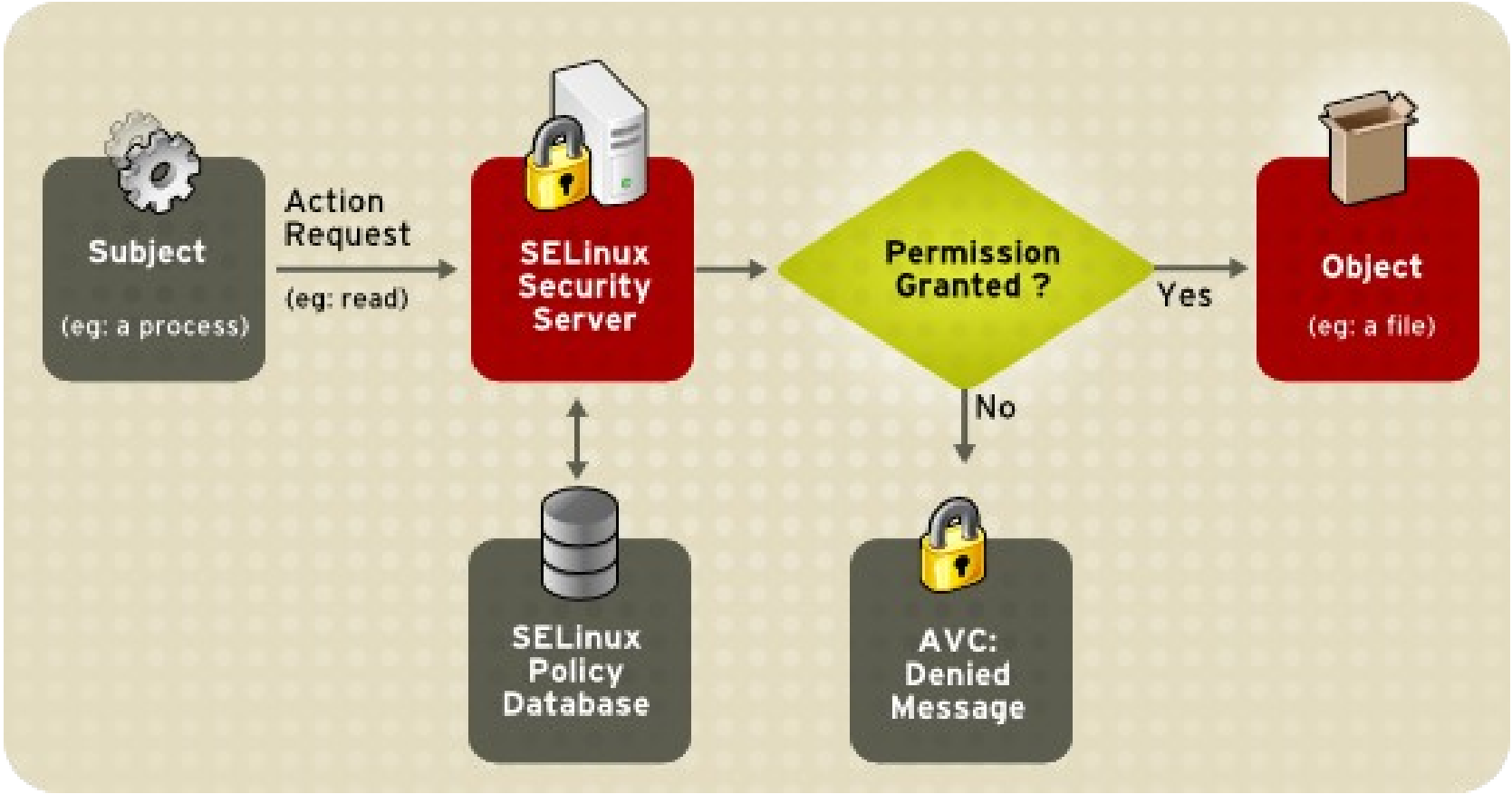
SELinux

- SELinux (Security Enhanced Linux) is one of the Linux features, which offers the component to supporting access control security policies.
- Its architecture provides general support for the implementation of several important access control policies, and also those that are based on the concepts of Multi Level Security, Type Enforcement and Role-Based Access Control.
- It is a Kernel security extension that can be used to prepare for compromised or misconfigured programs.

SELinux

- SELinux transition privileges and defines the access of each process, user, file and application on the system.
- On a regular basis, system users will be largely unaware of SELinux.
- Just system administrators need to consider how strict is the policy to implement for their server environment.

SELinux


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

Pluggable Authentication Modules (PAM)

- PAM is a system of libraries, which handles the authentication tasks of application on the system.
- It divides the tasks of authentication into four independent management groups:
  - Password management,
  - Session management,
  - Account management and
  - Authentication management.

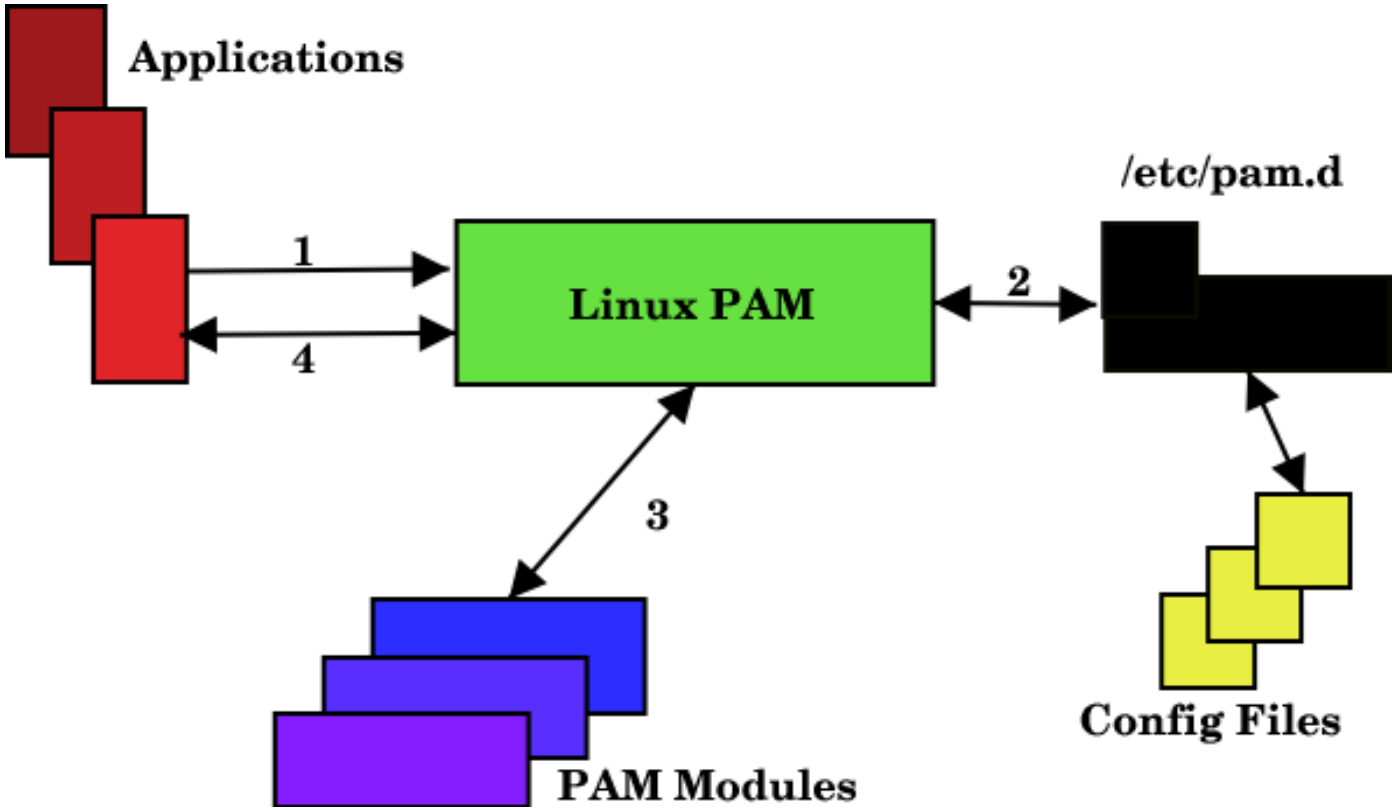
PAM

- Password:
  - This module interface is used for changing user passwords.
- Session:
  - This is used for managing and configuring user sessions.
  - It is very essential as it offers both closing and opening hook for modules to affect the services that are available to a user.
  - It can also perform other tasks that are expected to permit access, such as making the user's mailbox available and mounting a user's home directory.

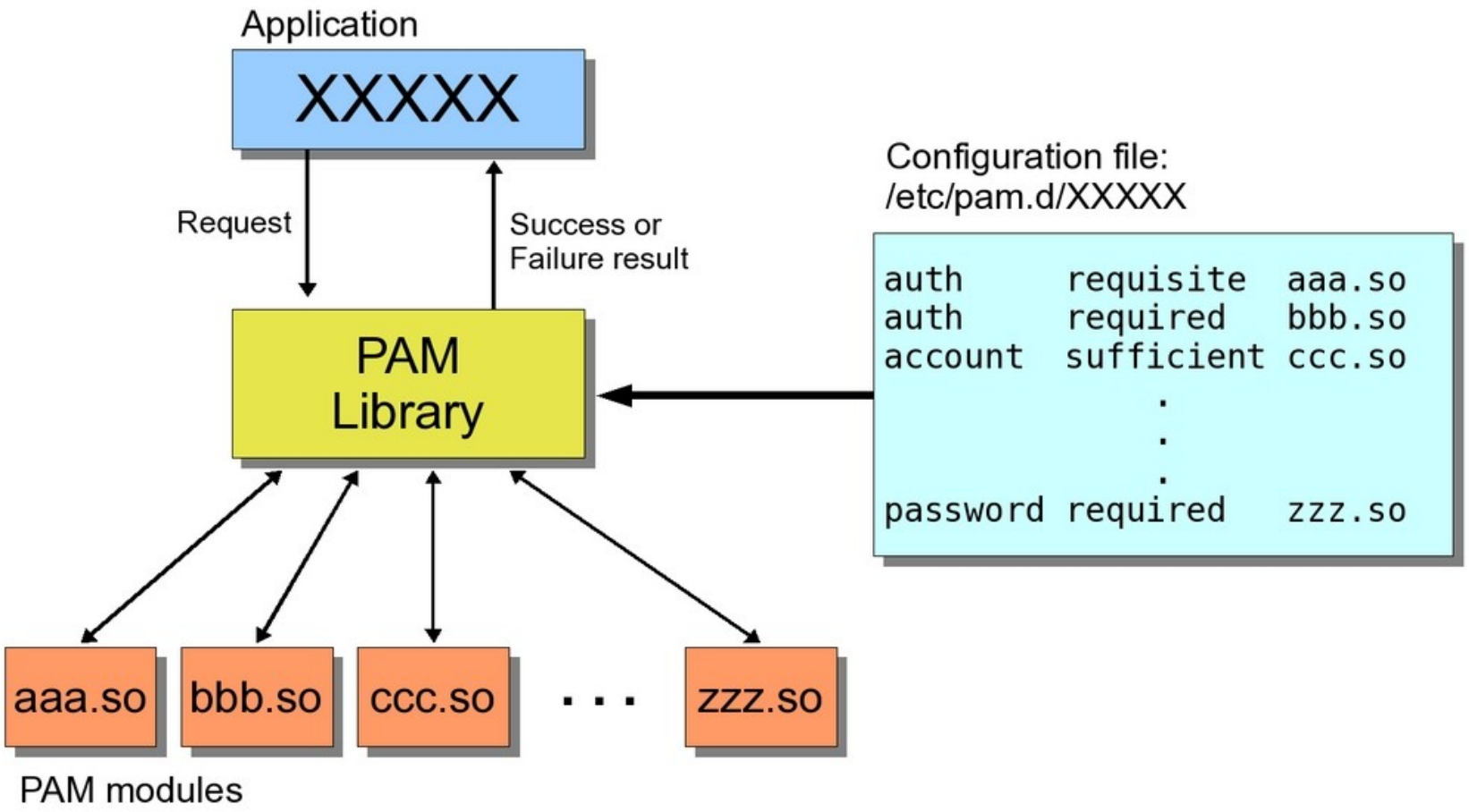
PAM

- Account:
  - It provides verification types of service such that it may check if a user is allowed to log in at a particular time of day or if a user account has expired.
- Authentication:
  - It can authenticate a user, such that it verifies and requests the validity of a password and set up user credentials such as Kerberos tickets or group memberships.

PAM


Applications
1
4
Linux PAM
2
/etc/pam.d
3
PAM Modules
Config Files

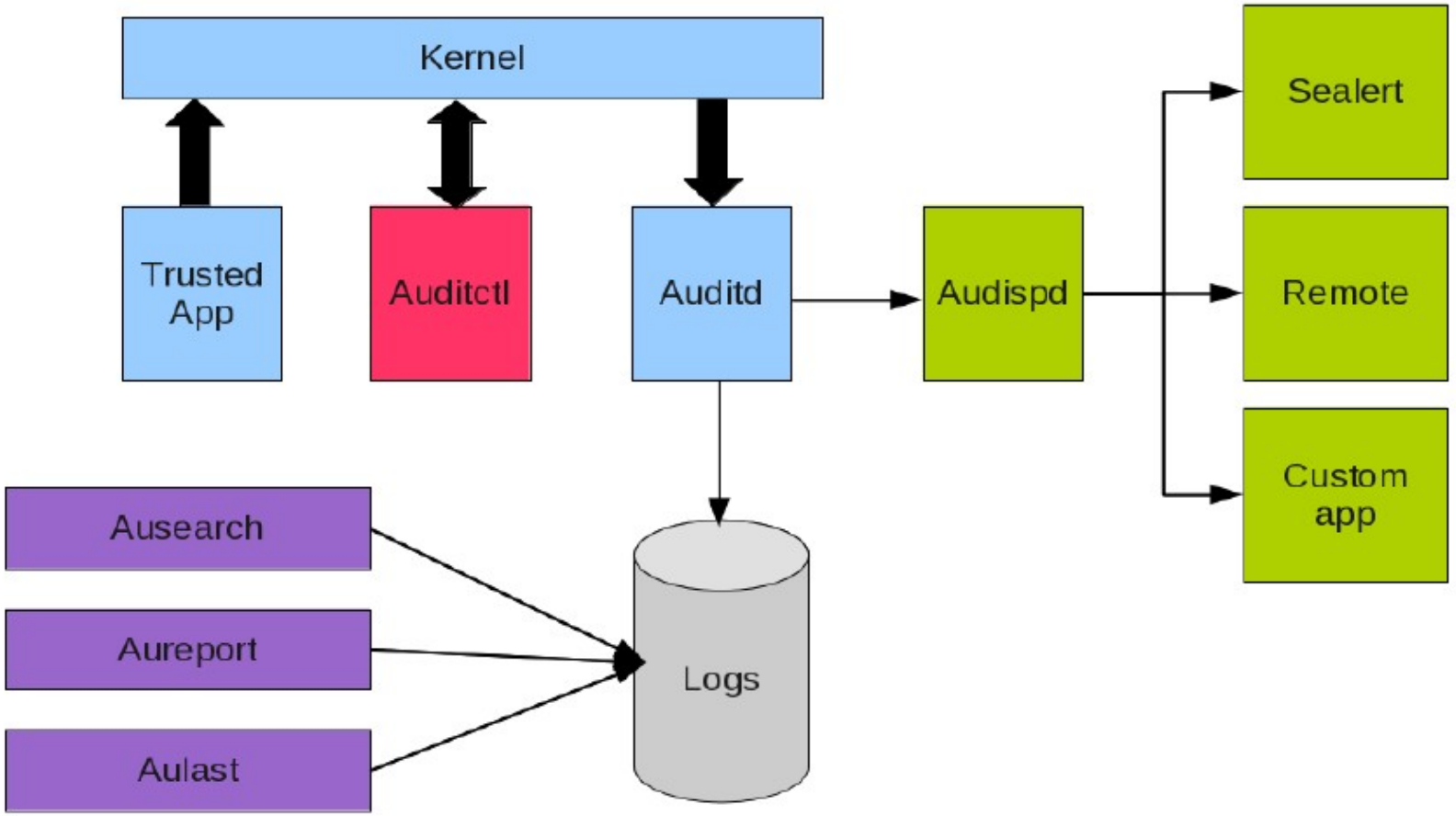
PAM


Application
XXXXX
Request
Success or
Failure result
PAM
Library
Configuration file:
/etc/pam.d/XXXXX
auth requisite aaa.so
auth required bbb.so
account sufficient ccc.so
.
.
.
password required zzz.so
aaa.so
bbb.so
ccc.so
. . .
zzz.so
PAM modules

Audit

- The Linux kernel can log events such as file access and system calls.
- These logs can be then be rechecked by the administrator to verify possible security concepts such as user failing to access system files or any failed login attempts. This functionality is known as Linux Auditing System.
- Auditd is the user space component of the Linux auditing system. Its work is to write audit records to the disk.
- When auditd runs the audit message sent by the kernel, it will be collected in the log file configured for auditd.
- For any reason, if auditd not runs, the kernel audit messages will be sent to rsyslog.

Audit


Kernel
Trusted App
Auditctl
Auditd
Audispd
Sealert
Remote
Custom app
Ausearch
Aureport
Aulast
Logs

Account Privileges

Account Privileges

- In Windows, by default users have access to everything in the system as they are given administrator rights.
- If the virus will enter their system, they can immediately gain access to significant parts of the system.
- Whereas in Linux, they have a lower access rights and virus can only access local files and folders, hence the system will remain safe.

Prime References

- *http://kerneltraining.com*
- *http://linux.com*
- *http://unixmen.com*

Thank you

Web Resources
http://mitu.co.in
http://tusharkute.com

Blogs
http://digitallocha.blogspot.in
http://kyamputar.blogspot.in

tushar@tusharkute.com