

# System Security

***Ashok T M***

IBM Linux Technology Center

# Agenda

- Installation - Hardening linux installation
- Patch Management- Updating linux system with latest security patches
- Physical Security – Restricting physical access to linux server
- Authentication -- Verifying users claimed identity is valid or not
- Isolation of services - Keeping services from impacting each other

# Hardening linux installation

❖ Key is to achieve secure Linux installation

- The media of the Linux distribution
- Minimize points of exposure.
- Install and secure the trusted features.
- Set up mechanisms to know about violations
- Update the Linux System with the latest security patches.

# Patch Management

- Updating the Linux system with the latest security patches
- Many vendors provide a patch management program which automates the process.  
Eg : RHN from Red Hat.

# Physical Security

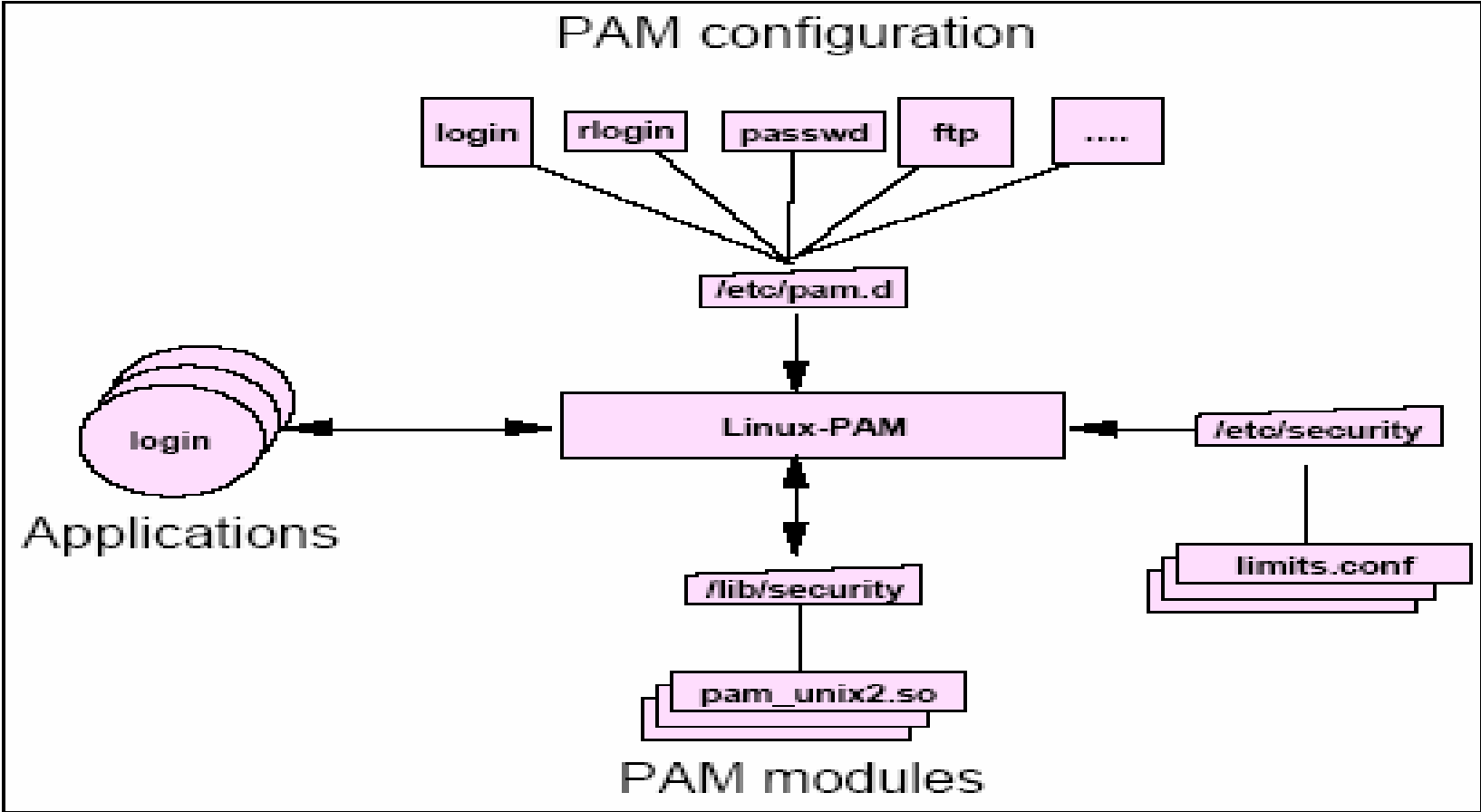
- Physically secure the servers
- Protect the system from undesirable booting
  1. BIOS password
  2. Boot loader password
- Use xlock and vlock
- Set up storage protection for backup tapes

# Authentication

## ❖ The Linux Way

- PAM - Pluggable Authentication Modules
- SASL- Simple Authentication and Security Layer
- Kerberos - An Authentication Protocol
- NIS+ - Network Information Service
- SSH - Secure Shell

# PAM Architecture

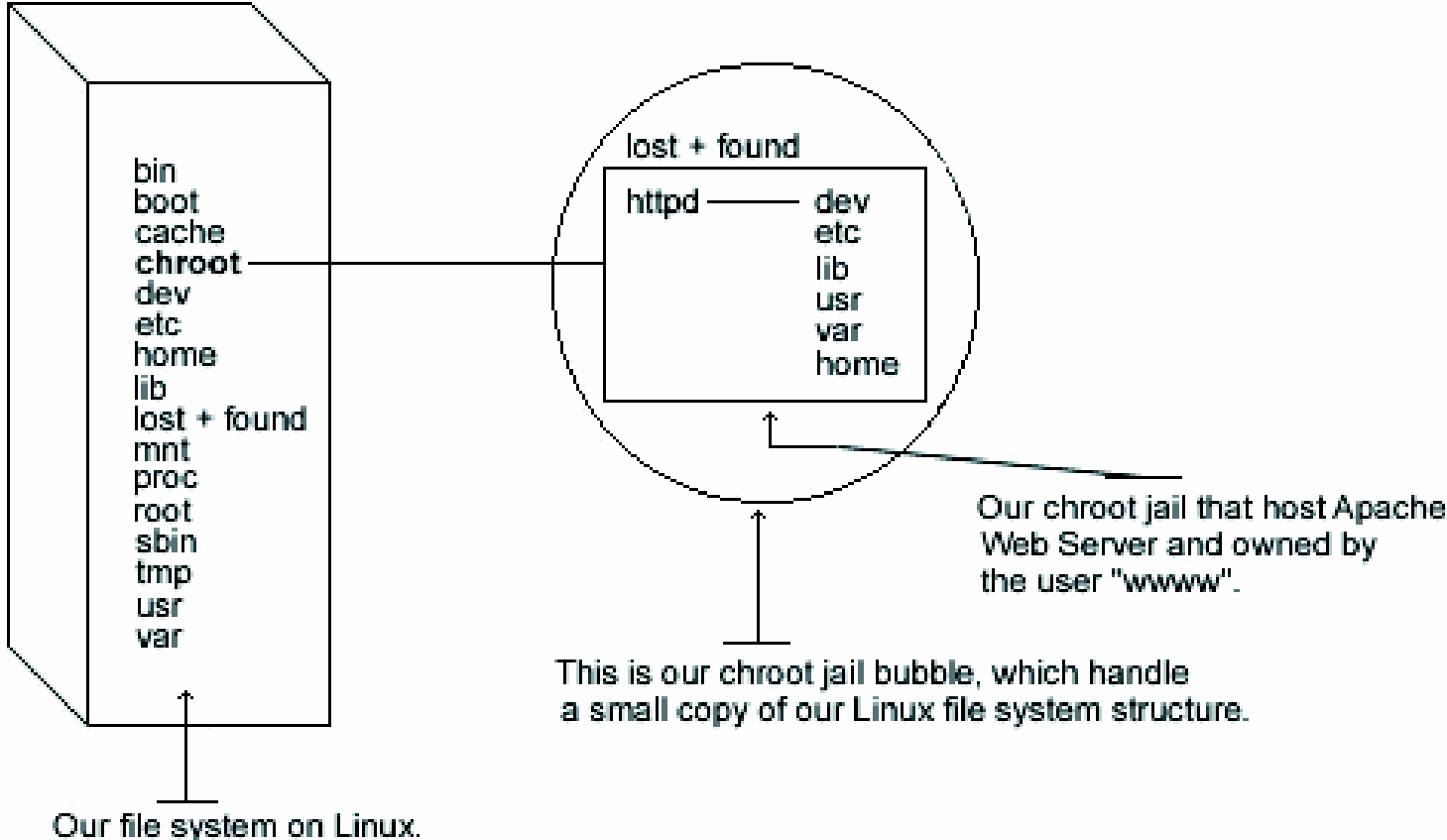


# Isolation of services

## ❖ The *chroot* jail

- A way to limit a process to a subdirectory
- Changes the 'file system root' for the process to be the subdirectory.
- Idea is limit the amount of access any malicious individual could gain by exploiting vulnerabilities in a process

# Chroot jail



# System Security

## ❖ Best Practices

- Authenticate users from a central repository to lower maintenance overhead.
- Maintain user password standards and expiration policies.
- Limit the number of users authorized to access the system.
- Limit the number of running services.

# Best practises

....contd

- Install and upgrade RPM packages from trusted sources.
- Logging to a central log server and log all system accesses.
- Apply recommended security patches to Linux hosts.
- Restrict the number of hosts running X Windows.
- Do not allow programming languages and compilers on production machines

- IBM and IBM(logo) are trademarks of International Business Machines Corporation in the United States, other countries, or both.
- Linux is trademark of Linus Trovalds
- Other company, product or service names may be trademarks or service marks of others.