Layered Security in CentOS 7

Operative Systems Class, Universidad Tecnologica de Pereira

2018 - 1

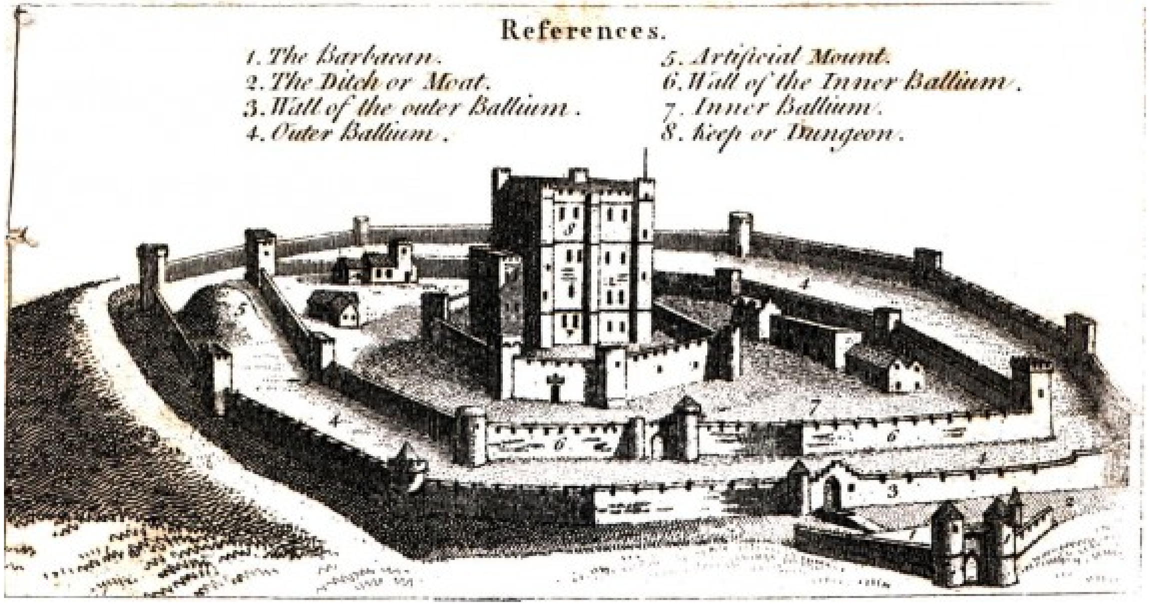
Created by Hector F. Jimenez S. and Cristian Ramirez

Content

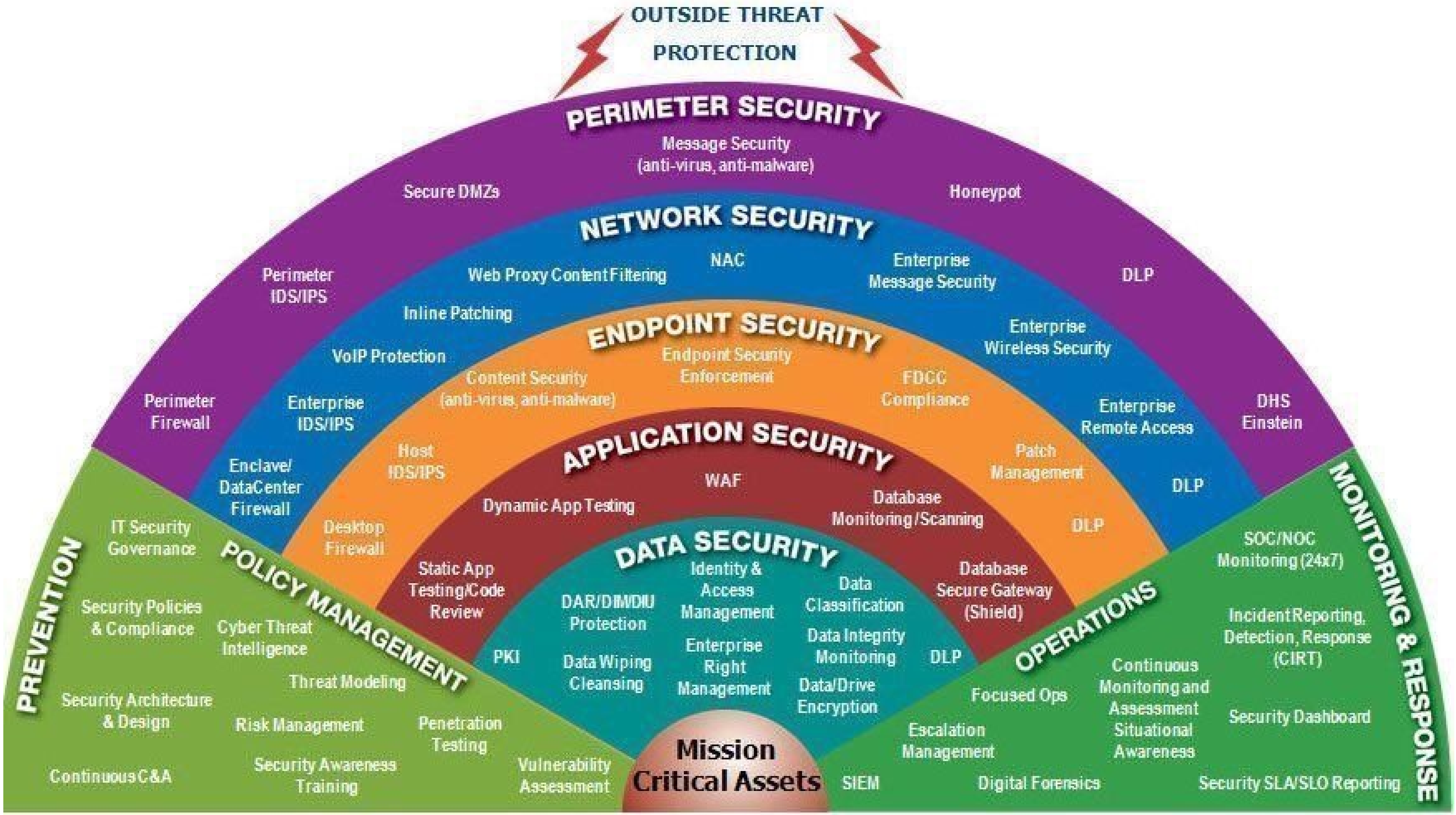
1. Security Context
2. Layered Security
3. CentOS Background
4. CentOS Security Review
5. Security Models

What is security?

Defense in depth and Layered Security



Now Defense in depth and Layered Security is



Security is not a product, is a process which try to reduce the surface attack

CentOS (Community ENTerprise Operating System)

Release Date

First release on May 14th 2004

Latest release on May 10th 2018

Distributions Related

Based on Red Hat Linux Enterprise

CentOS sponsored by Red Hat from 2014

Projects based on CentOS

System Hardening

The purpose of system hardening is to eliminate as many security risks as possible.

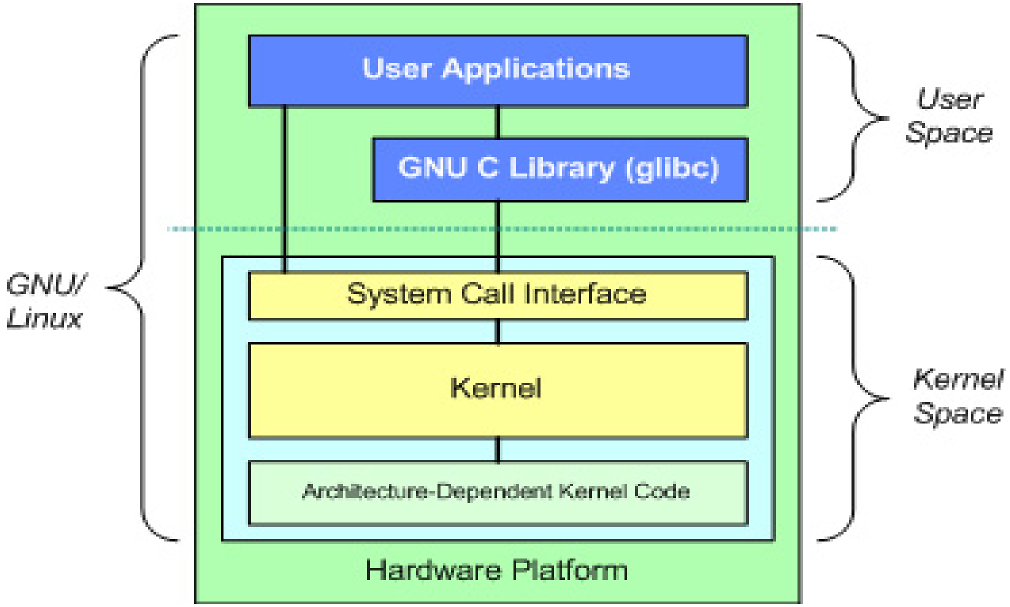
System Hardening

Installing extra software or running extra services creates unnecessary vulnerabilities

CentOS Security Model

[1] All the info here

CentOS Security Model



There're so many posibilities to ensure your System

Data Encryption

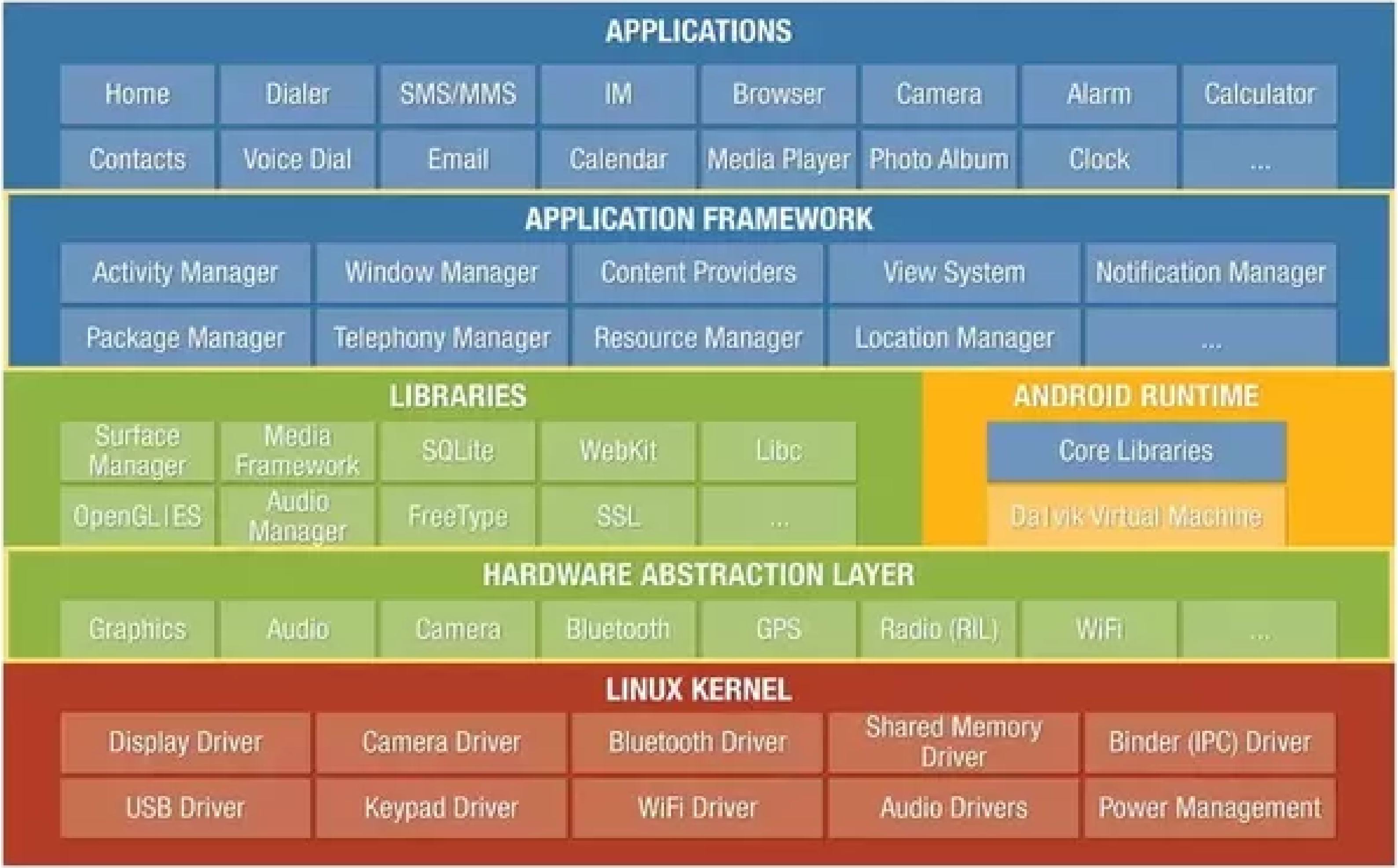
Data Security

FileSystem Security

Memory Protection

Service Protection

CentOS Security Model



APPLICATIONS

Home, Dialer, SMS/MMS, IM, Browser, Camera, Alarm, Calculator

Contacts, Voice Dial, Email, Calendar, Media Player, Photo Album, Clock, ...

APPLICATION FRAMEWORK

Activity Manager, Window Manager, Content Providers, View System, Notification Manager

Package Manager, Telephony Manager, Resource Manager, Location Manager, ...

LIBRARIES

Surface Manager, Media Framework, SQLite, WebKit, Libc

OpenGL|ES, Audio Manager, FreeType, SSL, ...

ANDROID RUNTIME

Core Libraries

Dalvik Virtual Machine

HARDWARE ABSTRACTION LAYER

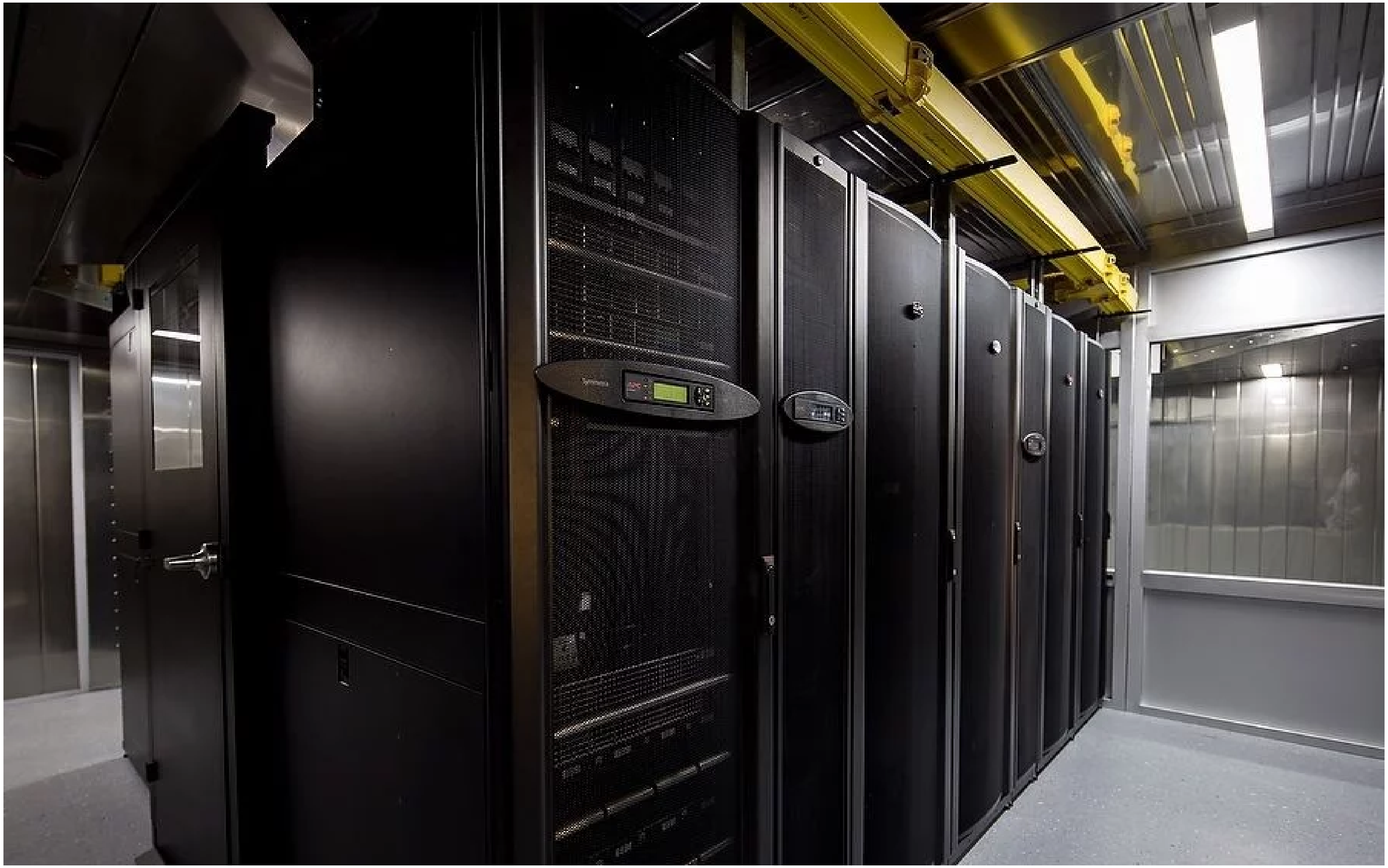
Graphics, Audio, Camera, Bluetooth, GPS, Radio (RIL), WiFi, ...

LINUX KERNEL

Display Driver, Camera Driver, Bluetooth Driver, Shared Memory Driver, Binder (IPC) Driver

USB Driver, Keypad Driver, WiFi Driver, Audio Drivers, Power Management

CentOS Phisycal Layer



CentOS Phisycal Layer

- BIOS protection
- Disable USB's or created a WhiteList

FileSystem

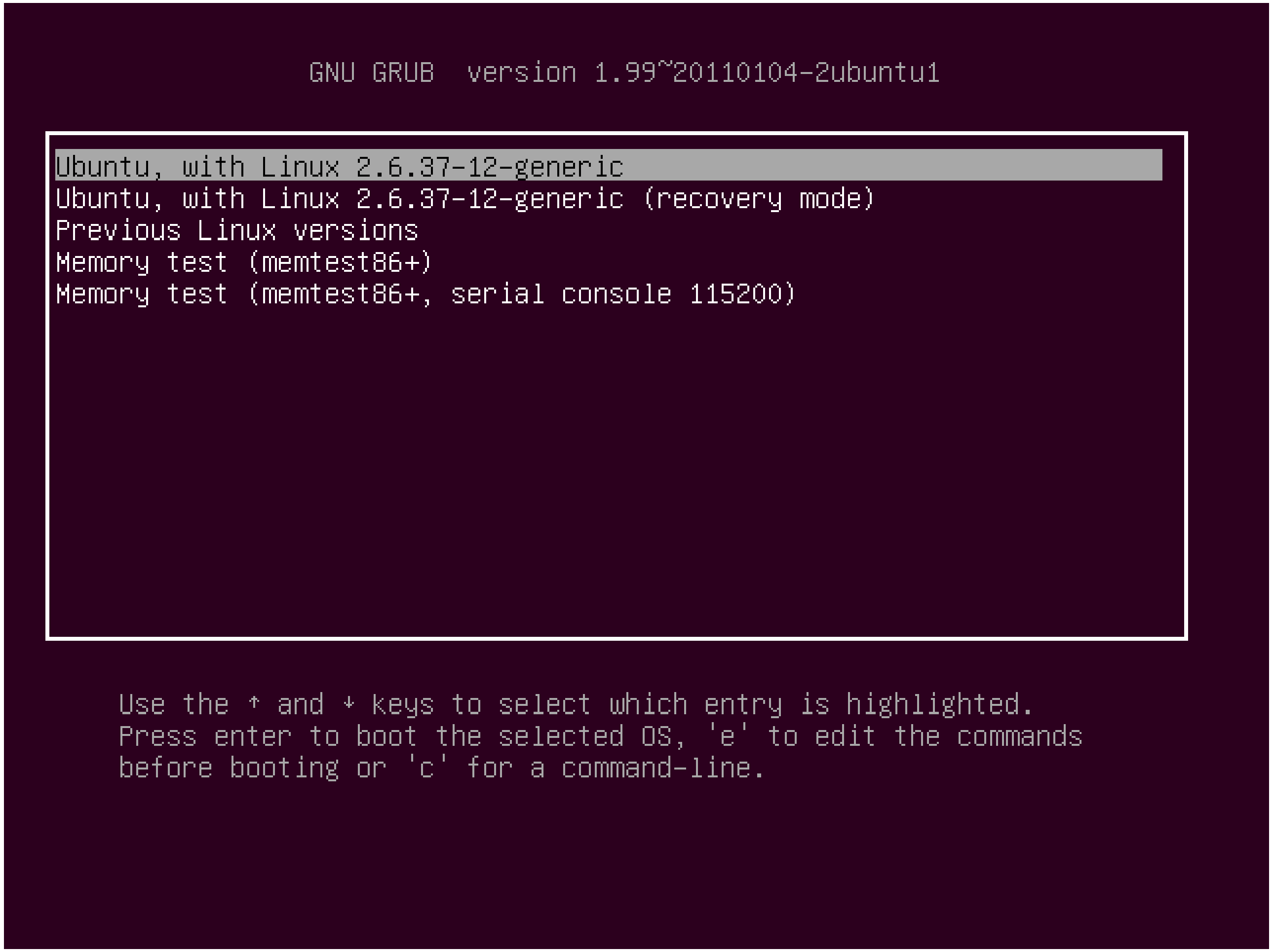
Partitioning

Partitioning is a key part of implementing security at the file system level.

1. It limits the impact of disk failure
2. It simplifies the process of creating backups
3. It allows administrators to add restrictions such as quotas and read-only permissions more effectively

```
/dev/VG_OS/lv_root          /        ext3      defaults     1 1
/dev/VG_OS/lv_tmp           /tmp     ext3      defaults,nosuid,no
/dev/VG_OS/lv_vartmp        /var/tmp ext3      defaults,nosuid,no
/dev/data_vol/lv_home       /home    ext3      defaults,nosuid,no
/dev/VG_OS/lv_var           /var     ext3      defaults,nosuid
/dev/data_vol/lv_web        /var/www ext3      defaults,nosuid,no
/dev/sda1                   /boot    ext3      defaults,nosuid,no
tmpfs                       /dev/shm tmpfs     defaults 0 0
devpts                      /dev/pts devpts    gid=5,mode=620 0 0
sysfs                       /sys     sysfs     defaults    0 0
proc                        /proc    proc      defaults    0 0
/dev/_VG_OS/lv_swap         swap     swap      defaults    0 0
```

Protect your Bootloader

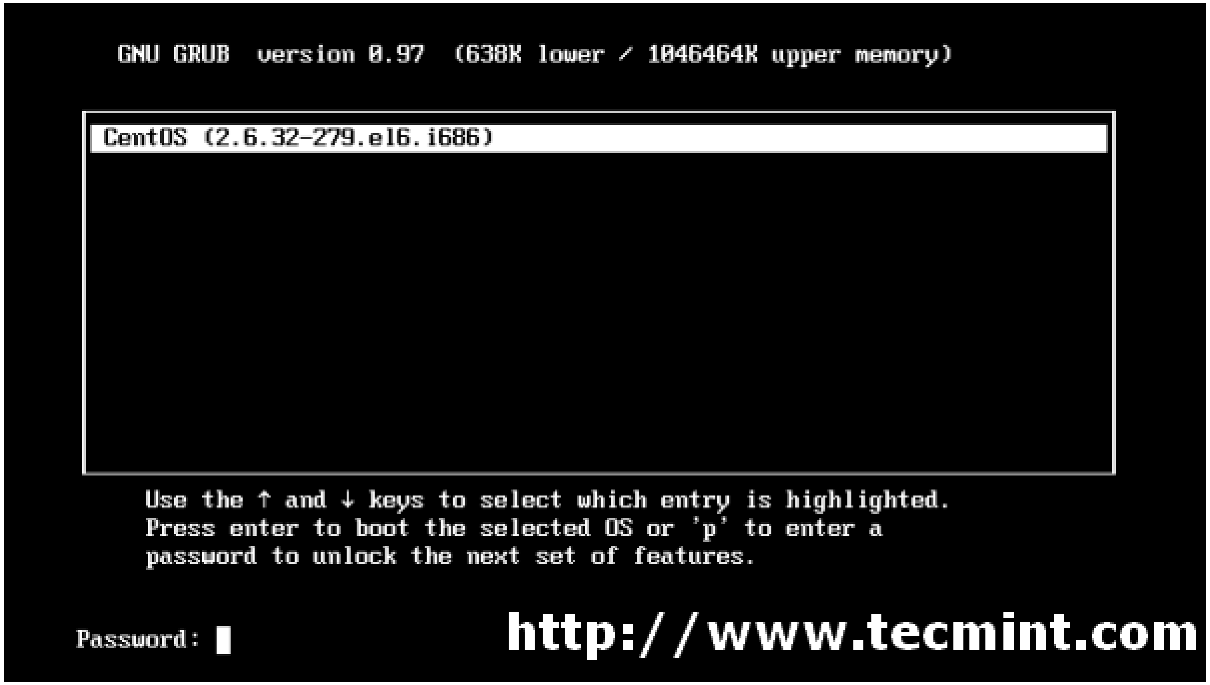


```
                 GNU GRUB  version 1.99~20110104-2ubuntu1

  Ubuntu, with Linux 2.6.37-12-generic
  Ubuntu, with Linux 2.6.37-12-generic (recovery mode)
  Previous Linux versions
  Memory test (memtest86+)
  Memory test (memtest86+, serial console 115200)

      Use the ↑ and ↓ keys to select which entry is highlighted.
      Press enter to boot the selected OS, 'e' to edit the commands
      before booting or 'c' for a command-line.
```

Protect your Bootloader



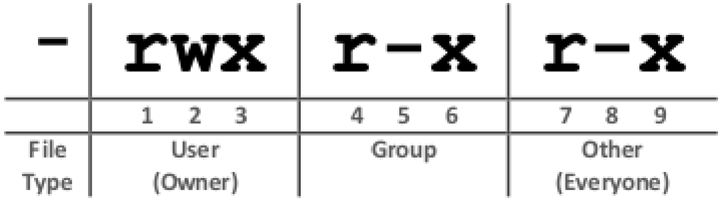
```
GNU GRUB  version 0.97  (638K lower / 1046464K upper memory)

CentOS (2.6.32-279.el6.i686)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS or 'p' to enter a
    password to unlock the next set of features.

Password: █
```

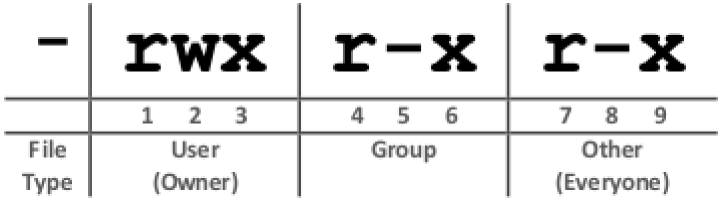
Protect your Bootloader



-	rwx	r-x	r-x
	1 2 3	4 5 6	7 8 9
File Type	User (Owner)	Group	Other (Everyone)

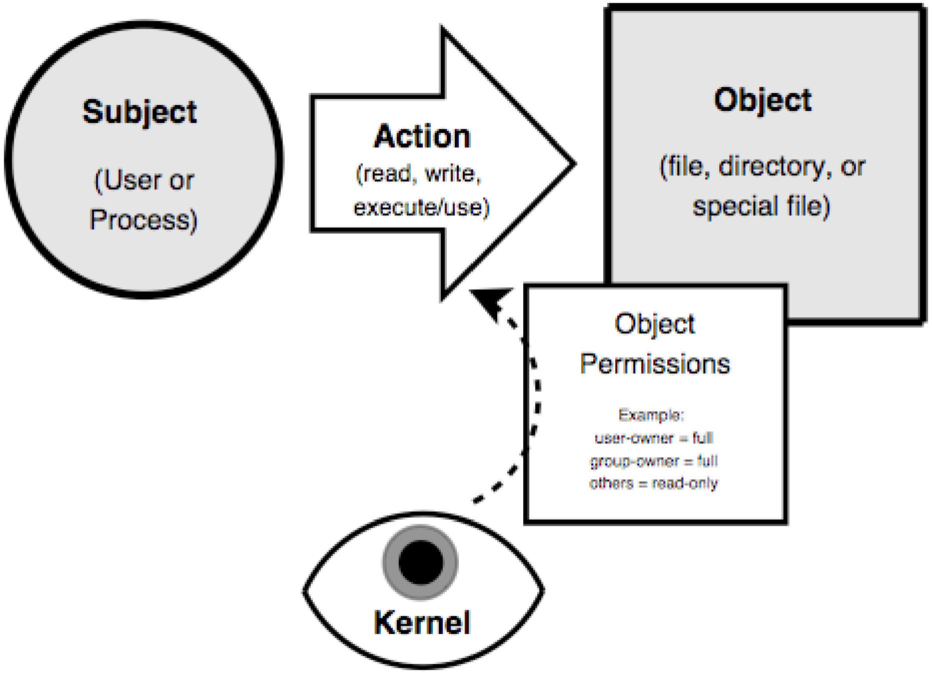
User and Group Permissions

Permissions



-	rwx	r-x	r-x
	1 2 3	4 5 6	7 8 9
File Type	User (Owner)	Group	Other (Everyone)

Security Models



Security Models

- in Linux everything as a file e.g. memory, device-drivers, named pipes, and other system resources hence why filesystem security is so important
- I/O to devices is via a “special” file, e.g. /dev/cdrom
- have other special files like named pipes, a conduit between processes/programs

Security Models

1. Mandatory Access Control
2. Discretionary Access Control
3. Rule-Based Access Control
4. Role-Based Access Control

An Overview of Access Control

The term Access Control actually refers to thecontrol over access to system resources after a user's account credentials and identity have been authenticated and access to the system granted.

control over access to system resources

For example, a particular user, or group of users, might only be permitted access to certain files after logging into a system, while simultaneously being denied access to all other resources

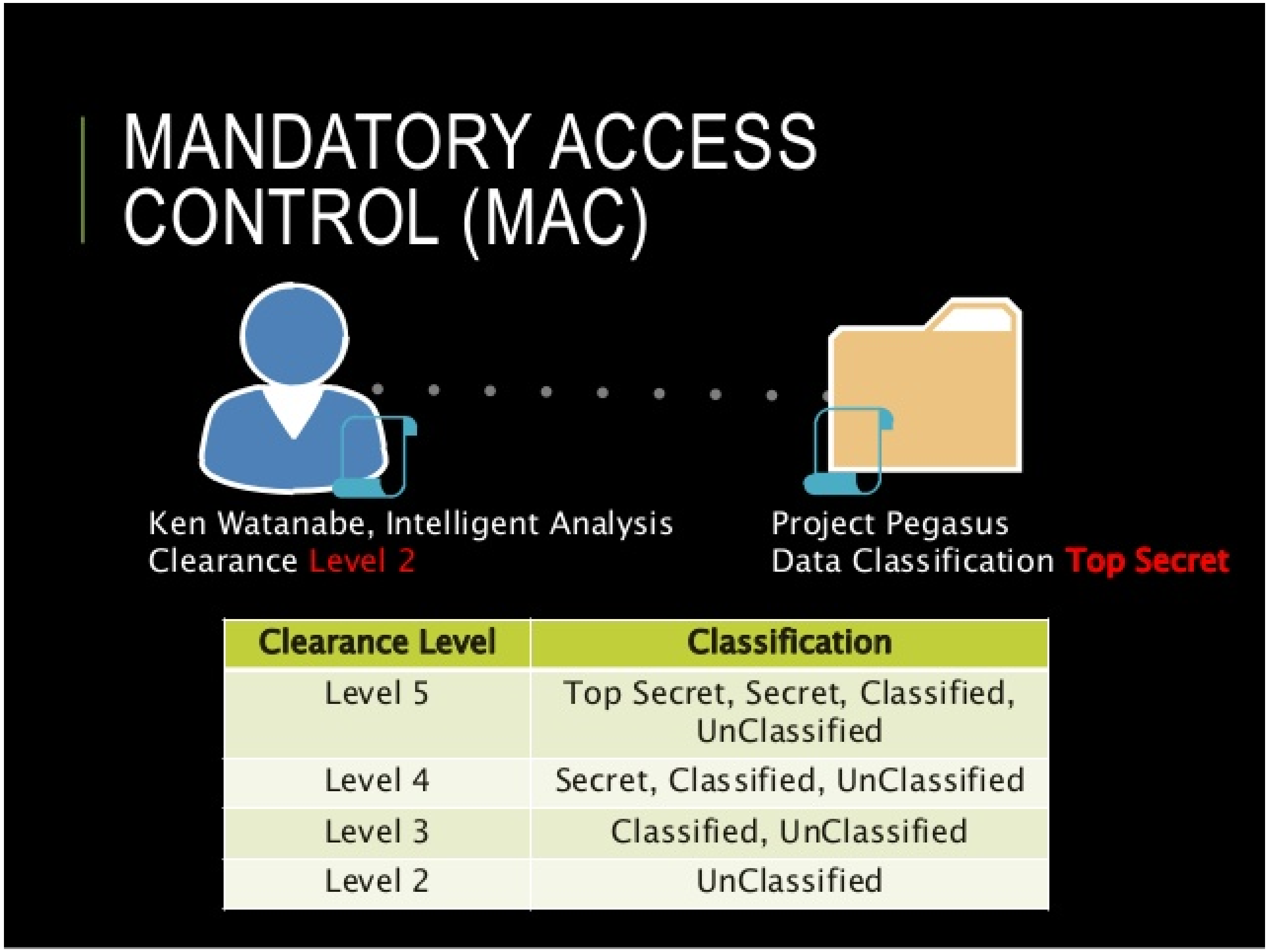
Mandatory Access Control (MAC)

takes a hierarchical approach to controlling access to resources. Under a MAC enforced environment access to all resource objects (such as data files) is controlled by settings defined by the system administrator.

Mandatory Access Control (MAC)

As such, all access to resource objects is strictly controlled by the operating system based on system administrator configured settings.

Mandatory Access Control (MAC)



MANDATORY ACCESS CONTROL (MAC)

Ken Watanabe, Intelligent Analysis
Clearance Level 2

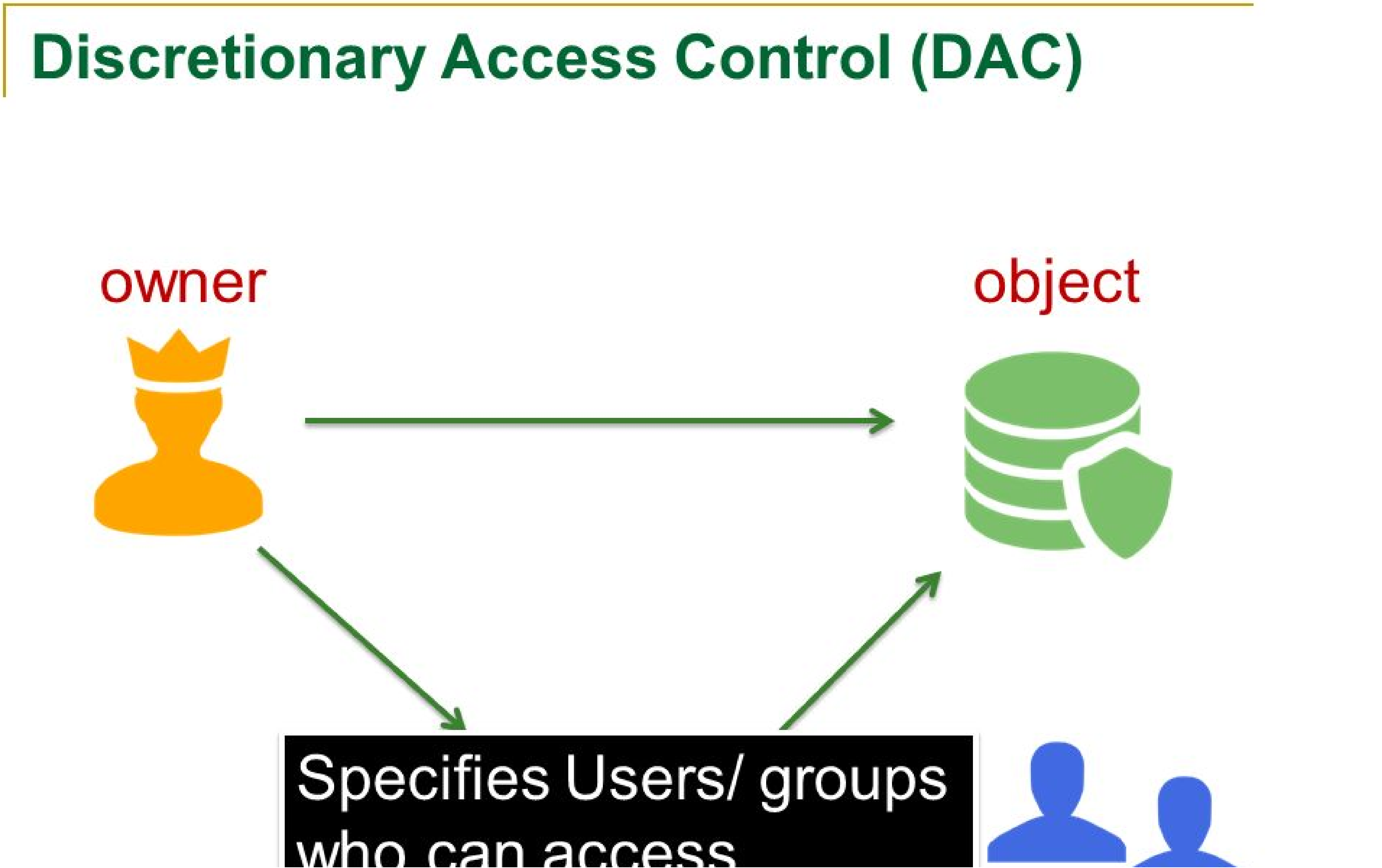
Project Pegasus
Data Classification Top Secret

Clearance Level	Classification
Level 5	Top Secret, Secret, Classified, UnClassified
Level 4	Secret, Classified, UnClassified
Level 3	Classified, UnClassified
Level 2	UnClassified

Discretionary Access Control (DAC)

Discretionary Access Control (DAC) allows each user to control access to their own data. DAC is typically the default access control mechanism for most desktop operating systems

Discretionary Access Control (DAC)



Discretionary Access Control (DAC)

Specifies Users/ groups who can access

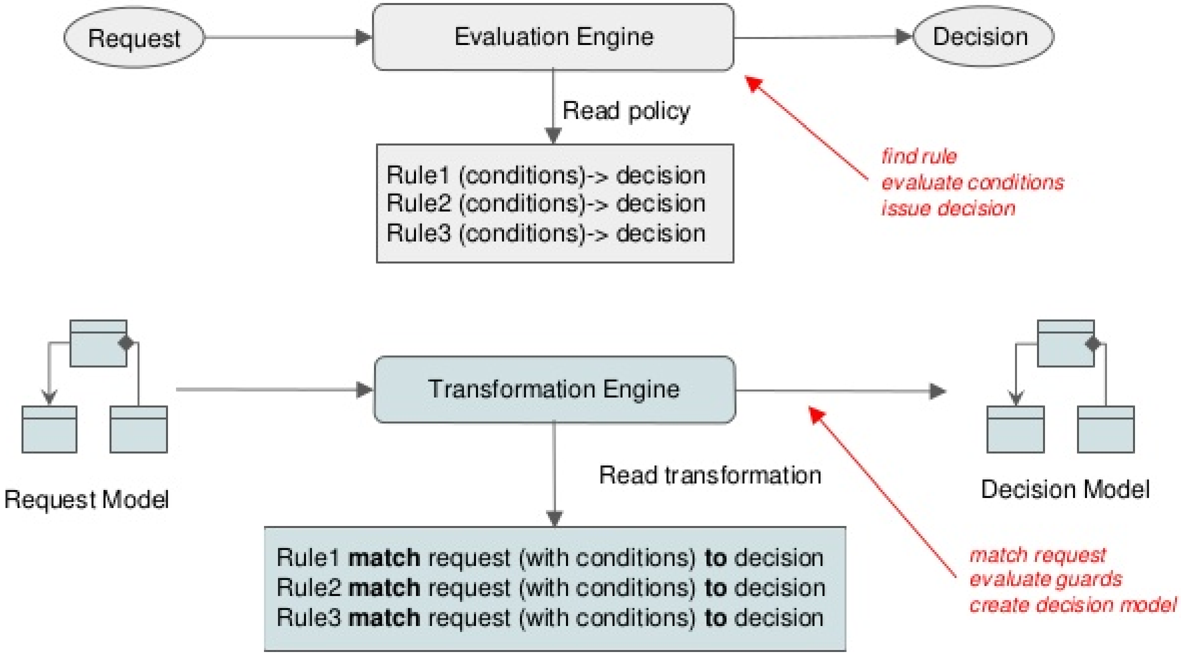
who can access

Rule-Based Access Control

1

Under Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator.

Rule-Based Access Control



Rule1 (conditions)-> decision
Rule2 (conditions)-> decision
Rule3 (conditions)-> decision

find rule
evaluate conditions
issue decision

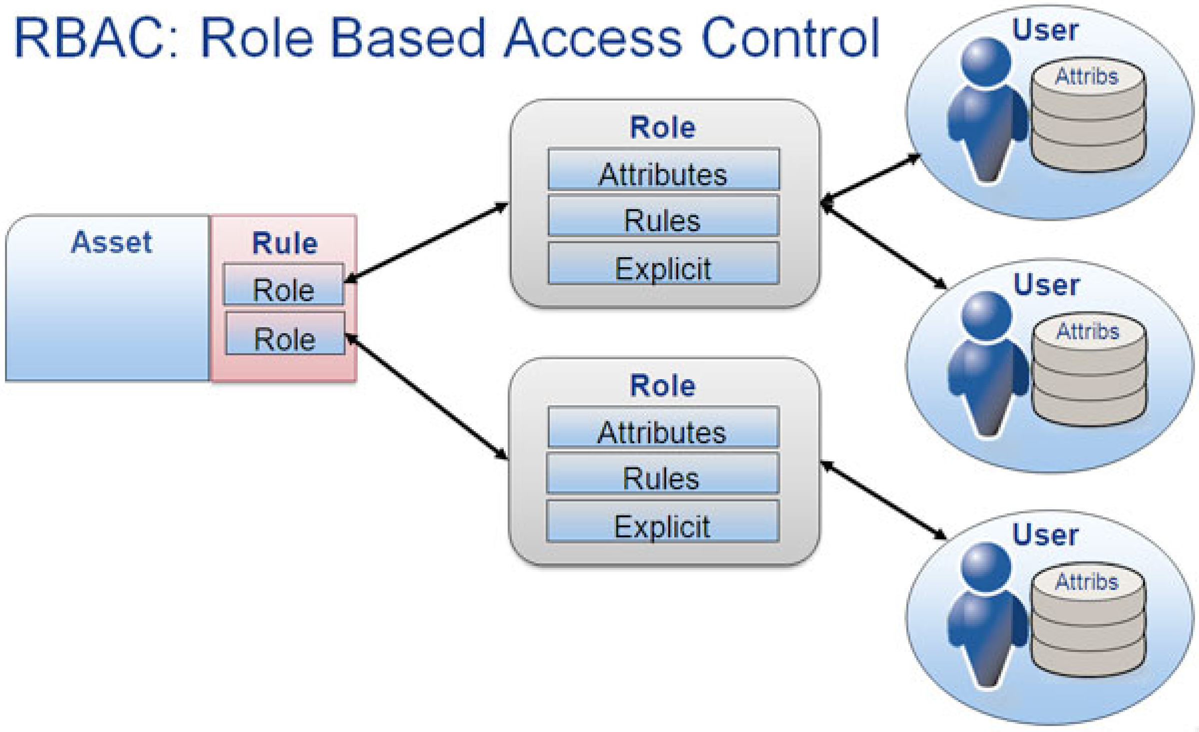
Rule1 **match** request (with conditions) **to** decision
Rule2 **match** request (with conditions) **to** decision
Rule3 **match** request (with conditions) **to** decision

match request
evaluate guards
create decision model

Role Based Access Control

Access under RBAC is based on a user's job function within the organization to which the computer system belongs. Essentially, RBAC assigns permissions to particular roles in an organization. Users are then assigned to that particular role

Role-Based Access Control


RBAC: Role Based Access Control
Asset
Rule
Role
Role
Role
Attributes
Rules
Explicit
Role
Attributes
Rules
Explicit
User
Attribs
User
Attribs
User
Attribs