Linux
Kullanıcıları
Derneği

SELinux'a Giriş

Emre Eryılmaz

emre.eryilmaz@linux.org.tr

Linux Kullanıcıları Derneği

2 Şubat 2012

Güvenlik Nedir?

- Güvenlik (Sistem ve Bilgi Güvenliği), elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.
- Güvenlik , en temelden(basit) seviyeden başlayıp en üst seviyeye(kompleks) kadar bir zincir gibi bütündür.

Güvenlik Prensipleri

- **Gizlilik** (Bilginin yetkisiz kişilerin eline geçmesinin engellenmesi)
- **Veri Bütünlüğü** (Gönderilen verinin alıcıya çıktığı haliyle ulaşmasıdır.)
- **Süreklilik** (Beklenen işi zamanında yapma,performans)
- Üç temel prensipten sonra *kayıt altında tutma,kimlik doğrulama,güvenirlik ve inkar edememe* şeklinde devam eder.

Güvenlik Prensipleri

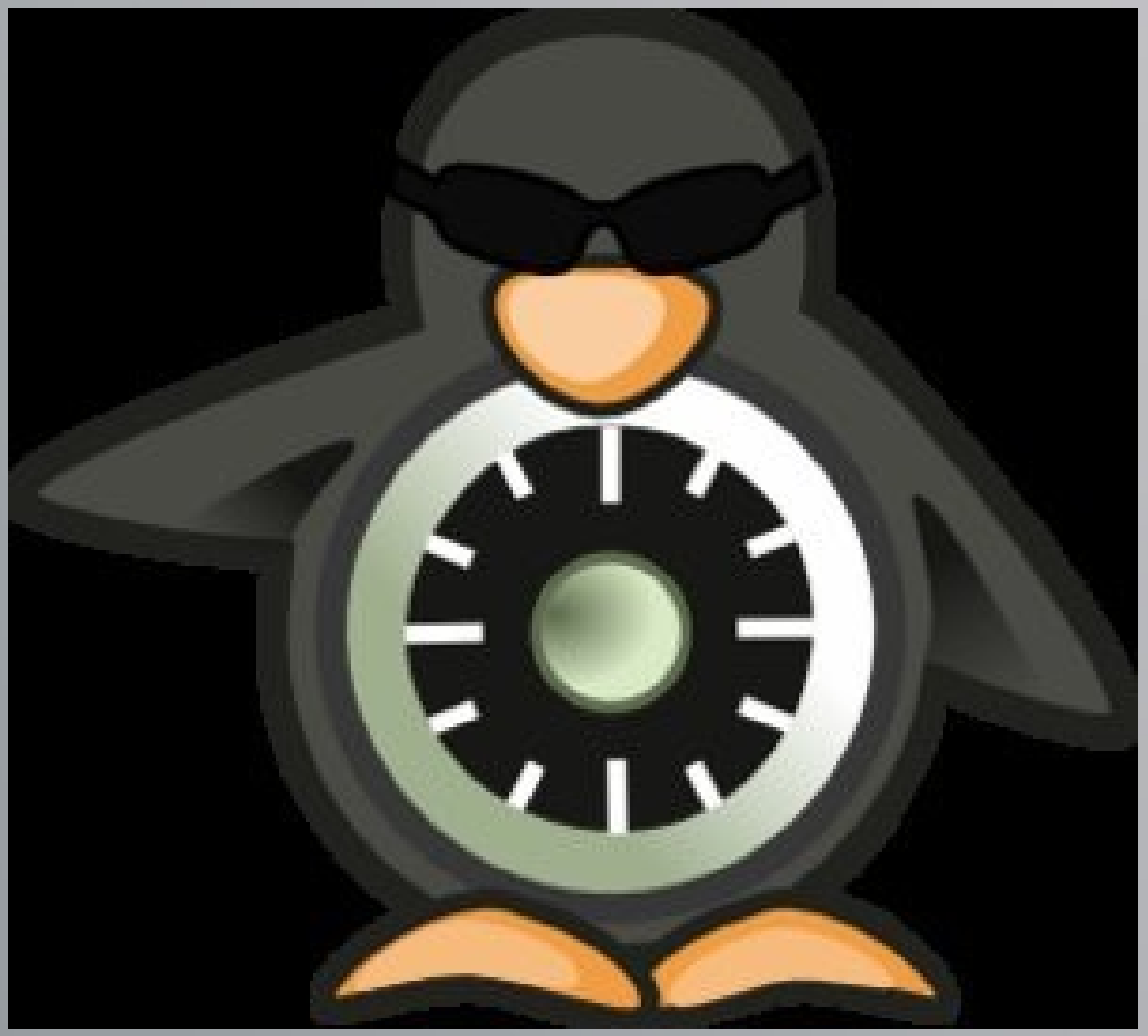
Erişim Kontrolü

- İyi bir erişim kontrolü sistemi(ya da sistemleri) sadece yetkili kişilerin ya da işlemlerin kaynağa erişimine izin verir.
- Fakat erişim kontrolünden önce de kimlik doğrulama sisteminin bulunması gerekir.
- Sağlıklı bir kimlik doğrulama mekanizması yok ise erişim kontrolü bir anlam ifade etmeyebilir.
- Linux üzerinde kimlik doğrulama mekanizması: PAM(Pluggable Authentication Modules)

Erişim Kontrolü

- Linux üzerinde kaynaklara erişimi yetkilendirme basit izin şemaları yapılır.
- Kaynakların çoğu varsayılan(default) olarak gizli değildir.
- Tehlike!! Esnek yetkilendirmeleri tam olarak tanımlamanıza izin vermez.(Öntanımlı olarak üç kullanıcı grubu kullanıcı,grup,diğerleri ve üç izin şekli okuma,yazma,çalıştırma)
- Sakınca!!İzin şemaları kullanıcıların isteğine bağlıdır.

SELinux'a Doğru



SELinux'a Doğru

- SELinux olarak bilinen Security-Enhanced Linux, Linux’a güvenlik açısından hangi ekstra özelliklerin eklenebileceğinin bir araştırması olarak, geliştirilmiş güvenlik özellikleri ve zorunlu giriş kontrolleri içeren ve Linux Kernel'in (Linux çekirdeğinin) ön ürünü olarak piyasa sunulan bir çekirdek yapısıdır. SELinux ilk olarak National Security Agency(NSA) tarafından 1999 yılında askeri projelerde kullanılmak üzere ordu için geliştirilmiştir. Sonrasında SELinux eklentisi, 2.6 serisi çekirdekler ile birlikte Linux çekirdeğine eklenmiştir.

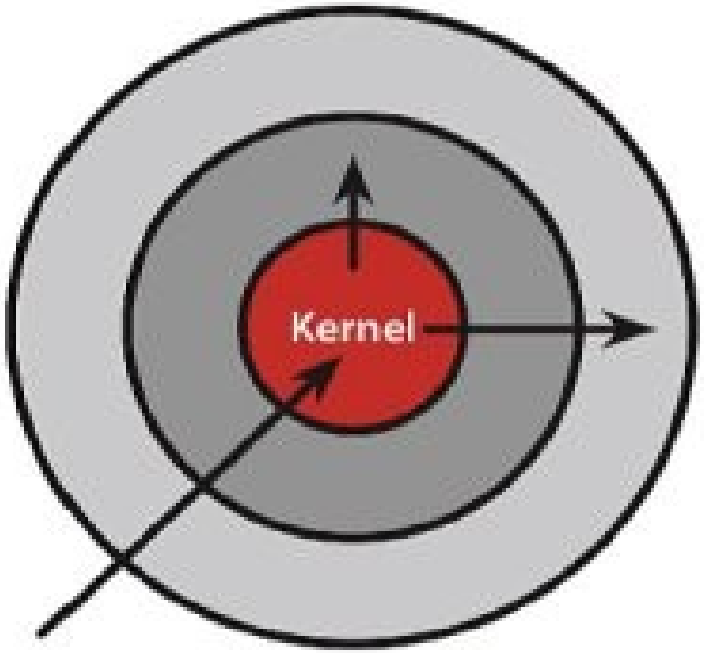
SELinux'a Doğru

- “ İsteğe Bağlı Erişim Kontrolü” nü(Discretionary Access Control – DAC) yeterli bulmadıysanız! (sözkonusu > güvenlik) “Zorunlu Erişim Kontrolü”ne (Mandatory Access Control – MAC) ihtiyaç duyacaksınız.
- Geleneksel Unix modelinden yani DAC ile kaynaklara erişim denetimi sadece kullanıcı kimliği ve nesne sahipliği sınanır.DAC'tan MAC'a

MAC(Mandatory Access Control)

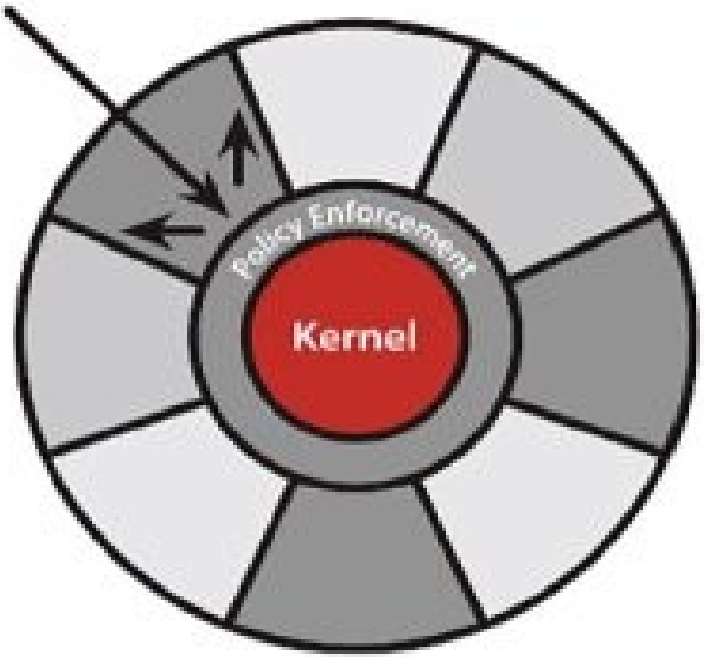
- Aktif bir işlem kendi kaynakları dışında bir kaynağa erişim ihtiyacı duyduğunda mutlaka izin verilmesi gerekir.
- Sadece dosya ve dizinleri değil,soketleri,portları,bellek segmentlerini,kuyrukları(queues),işlemleri(process),kernel hizmetlerini,sistem çağrılarını,aygıtları,dosya sistemlerini vs. bunları ve daha fazlasını destekler.
-

DAC vs. MAC



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.



Mandatory Access Control

Kernel policy defines application rights, firewalling applications from compromising the entire system.

Dosyalar için (MAC)

- Append
- Create
- Write
- Get- and setattr
- Read
- Rename
- Lock
- .....

Socketler için (MAC)

- Append
- Bind
- Connect
- Create
- Write
- Sendto
- Accept
- ....

SELinux Kavramları

- **Targeted policy** (Belirli process'leri kısıtlar.Daemon sonlandırır.)
- **Strict Policy** (Tüm process'leri sınırlandırır.Sınırlandırılmamış process kalmaz.)
- **Multi-Category Security Policy**(MCS) : Kısıtlanmış alanların sınıflandırılabildiği politikadır.

SELinux Kavramları

- Multi-Level Security Policy(MLS): Alanların ve kaynakların duyarlılığına ilişkin kuralların var olduğu politikadır.Bu uygun bir bilgi akışı politikası sağlar.

Güvenlik Bağlamları/Şartları

- Bunlar Kullanıcılar(users),Roller(roles),Alanlar(Domains),Duyarlılıklar(Sensitivities) ve Kategoriler(category)

User : Kaynağa atanan herhangi bir SELinux kullanıcısı.

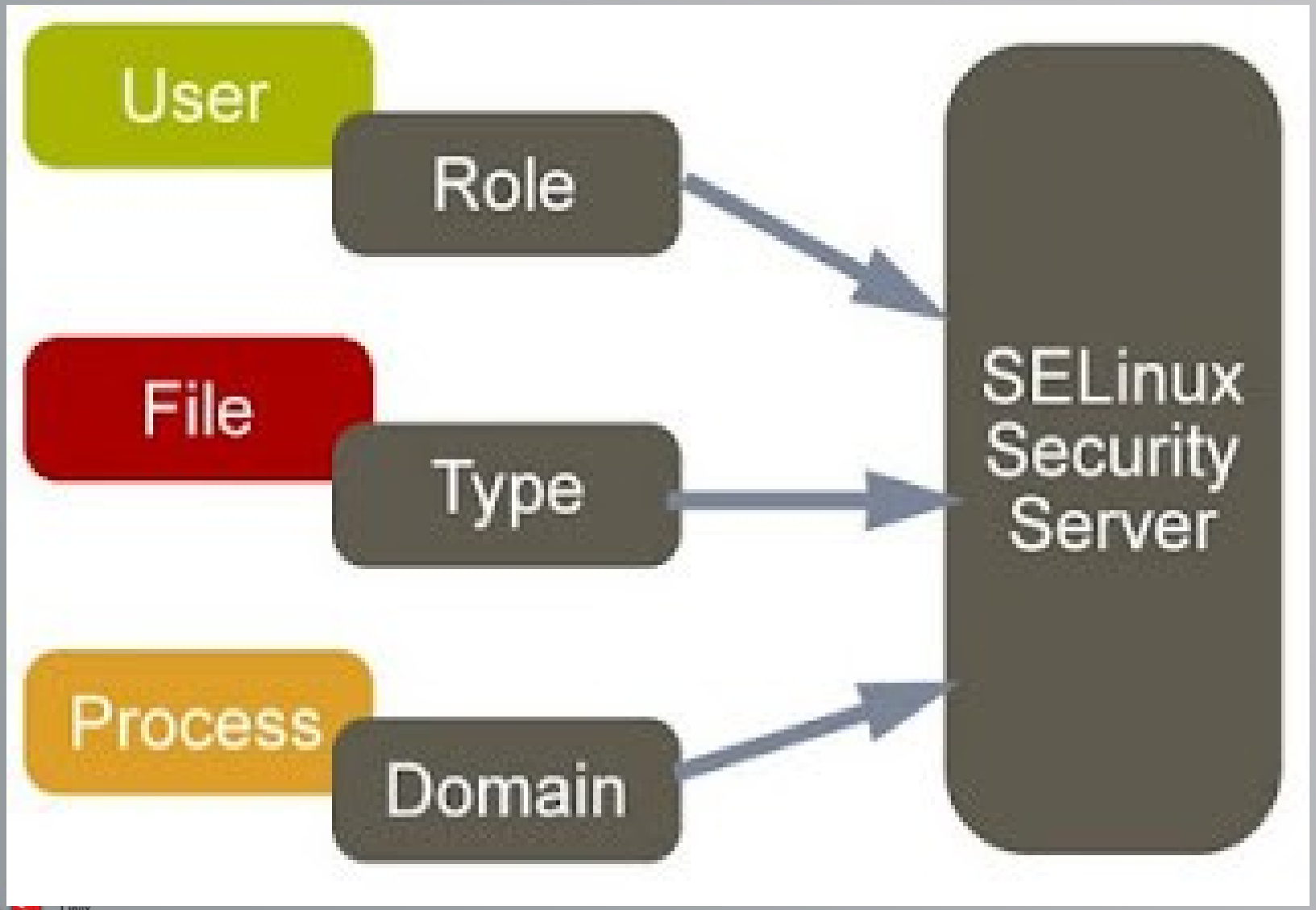
Role: Kaynağın şu anda çalıştığı SELinux rolü.

Type: Kaynağa atanan ve SELinux uygulama kurallarının anahtarı olan tür ya da modeldir.

Güvenlik Bağlamları/Şartları

- Sensitivity: Kaynağın duyarlılığı hakkında sistemi bilgilendiren kaynağa verilmiş olan seviyedir.Duyarlılık Public,Internal,Restricted,Confidential,Strictly Confidential gibi değerlerdir.
- Category: Bu kaynağın belirli bir örneklemesidir.Aynı tip olsalar bile kaynaklarımını sağlar.Kategoriler MLS ve MCS içinde desteklenir.

Güvenlik Bağlamları



Örnek bir güvenlik bağlamı:

```
~$ id -Z
staff_u:staff_r:staff_t
```

- *staff_u* : Selinux kullanıcısı
- *staff_r*: *staff_u* kullanıcısı *staff_r* rolünde
- staff_t: *staff_t* tipine atanmış.

Örnek bir güvenlik bağlamı:

```
~$ id -Z
staff_u:staff_r:staff_t:s0-s0:c0.c1023
```

- MCS(Multi-category Security) örneği
- S0 duyarlılık düzeyinde
- C0'dan c1023'e kadar olan kategori düzeyi
- Kategori isteğe bağlı

Erişim Kontrol Politikası

- Güvenlik bağlamları erişim kontrolü için gerekçedir.
- SELinux,kullanıcının güvenlik bağlamı ile erişmek istediği kaynağın izinleri kontrol eder.
- Kaynak tipleri nesne sınıflarından oluşur.
- Örnek nesne sınıfları:dosyalar,dizinler,process'ler,tcp_socketleri vs vs.

Örnek Erişim İzinleri

```
~# ls /selinux/class/process/perms
dyntransition  getcap      rlimitinh     setpgid         siginh
execheap       getpgid     setcap        setrlimit       sigkill
execmem        getsched    setcurrent    setsched        signal
execstack      getsession  setexec       setsockcreate   signull
fork           noatsecure  setfscreate   share           sigstop
getattr        ptrace      setkeycreate  sigchld         transition
```

- Process nesne sınıfının desteklemekte olduğu izinler.

SELinux Erişim Kontrol Kuralı

```
allow ACTOR  TARGET:CLASS PRIVILEGE;
      +-+-+  +-+--+ +-+-+ +---+---+
        |      |      |       `- Verilmiş olan izin ("yazma" gibi)
        |      |      `- İzin verilen Nesne Sınıfı ("dosya" gibi)
        |      `- Geçerli izinin olduğu kaynak ("portage" dizini gibi)
        `- Domain üzerinde ayrıcalık verilen aktör ("sysadm_t" gibi)
```

Örnek SELinux Kuralı

```
(Örnek olarak kullanıcının ev dizinin güvenlik bağlamlarını ekrana
yazdıralım.)
~$ ls -dZ ${HOME}
staff_u:object_r:user_home_dir_t  /home/swift

(staff_t tipindeki staff_u kullanıcısının user_home_dir_t tipindeki ev
dizinine yazma izninin olup olmadığını bulalım.)
~$ sesearch -s staff_t -t user_home_dir_t -c dir -p write -A
Found 1 semantic av rules:
  allow staff_t user_home_dir_t : dir { ioctl read write create ... };
```

- Örnekte görüldüğü gibi kullanıcı ev dizinine yazma iznine sahiptir.

Örnek SELinux Kuralı

```
~$ id -a
uid=1001(swift) gid=100(users) groups=100(users),...,250(portage),...
~$ ls -ldZ /var/tmp/portage
drwxrwxr-x. 3 portage portage  system_u:object_r:portage_tmp_t 4096 Dec  6
21:08 /var/tmp/portage
```

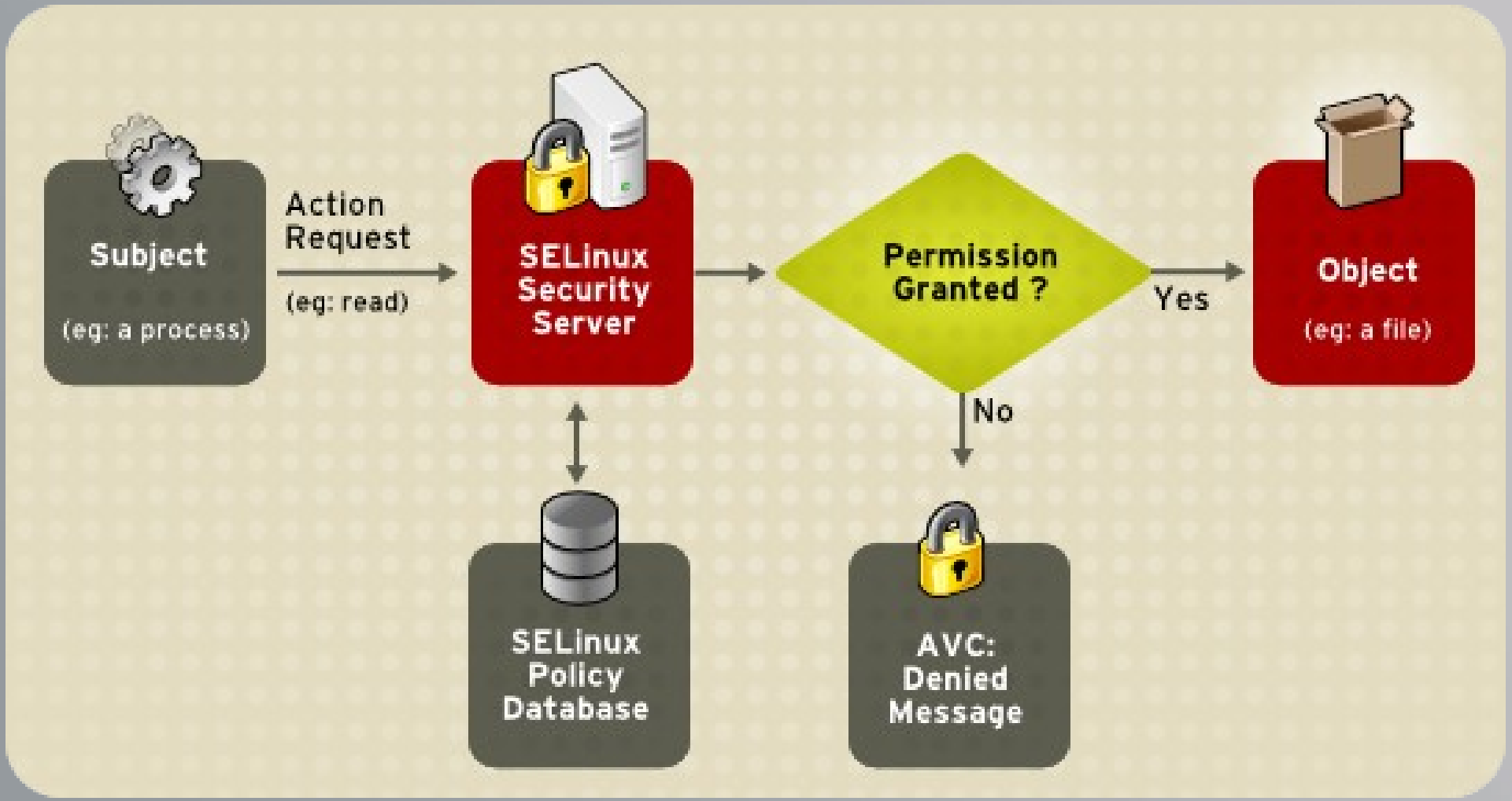
- Yukarda örnekte görüldüğü gibi kullanıcının portage grubunda ve bu grup “/var/tmp/portage” dizinine yazma hakkına sahip.
- Dikkat: Dosya ve Dizinlerin rolleri yoktur.Nesne sınıfları vardır.

SELinux buna ne der?

```
~$ sesearch -s staff_t -t portage_tmp_t -c dir -p write -A
~$
(Arama sonucunda hiçbir sonuç görüntülenemedi.)
~$ touch /var/tmp/portage/foo
touch: cannot touch '/var/tmp/portage/foo': Permission denied
```

- Unix erişim izinlerine göre yazma hakkı olmasına rağmen SELinux buna izin vermedi.Neden?
- staff_t domaini portage_tmp_t tipine izin verdi yetki görüntülenemedi.

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

SELinux hakkında bilgi:

- # getenforce
- # setenforce
- # setenforce 0 (oturum süresi boyu kapalı)
- # setenforce 1 (Tekrar devreye alır)

Linux
Kullanıcıları
Derneği