MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(6. Hafta)

İçerik

- 2.Yönetim Sorunları
  - 2.1. BT Güvenlik Yönetimi ve Risk Değerlendirmesi
  - 2.2.BT Güvenlik Kontrolleri, Planları ve Prosedürleri
  - 2.3.Fiziksel ve Altyapı Güvenliği
  - 2.4. İnsan Kaynakları Güvenliği
  - 2.5. Güvenlik Denetimi
  - 2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.5.Güvenlik Denetimi

2.5.İçerik

- Güvenlik Denetim Mimarisi
- Güvenlik Denetimi İzi
- Loglama İşlevini Uygulama
- Denetim İzi Analizi
- Güvenlik Bilgileri ve Olay Yönetimi

Güvenlik Denetimi Terminolojisi (RFC 4949)

Güvenlik Denetimi	Sistem kontrollerinin yeterliliğini belirlemek, yerleşik güvenlik politikası ve prosedürlerine uyumu sağlamak, gizlilik hizmetlerindeki ihlalleri tespit etmek ve karşı önlemler için belirtilen değişiklikleri tavsiye etmek için bir sistemin kayıtlarının ve faaliyetlerinin bağımsız olarak gözden geçirilmesi ve incelenmesidir Temel denetim amacı, güvenlikle ilgili olayları ve eylemleri başlatan veya bunlara katılan sistem varlıkları için hesap verebilirlik oluşturmaktır. Bu nedenle, bir güvenlik denetim izi oluşturmak ve kaydetmek ve saldırıları ve güvenlik ihlallerini keşfetmek ve araştırmak için denetim izini incelemek ve analiz etmek için araçlara ihtiyaç vardır.
Güvenlik Denetimi İzi	Başlangıcından nihai sonuçlarına kadar güvenlikle ilgili bir işlemde bir operasyon, prosedür veya olayı çevreleyen veya bunlara yol açan ortamlar ve faaliyetler dizisinin yeniden oluşturulmasını ve incelenmesini sağlamak için yeterli olan sistem faaliyetlerinin kronolojik kaydıdır.

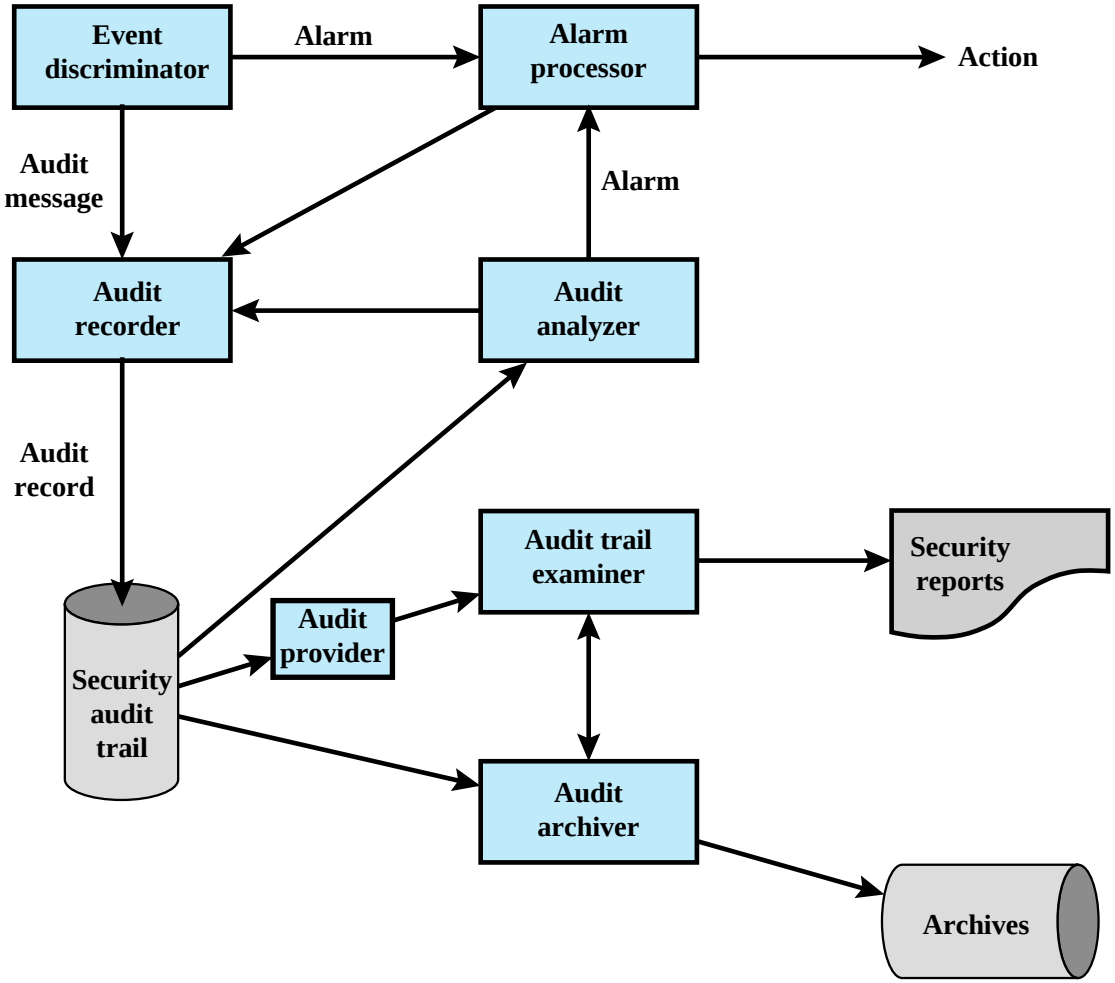


Figure 18.1 Security Audit and Alarms Model (X.816)

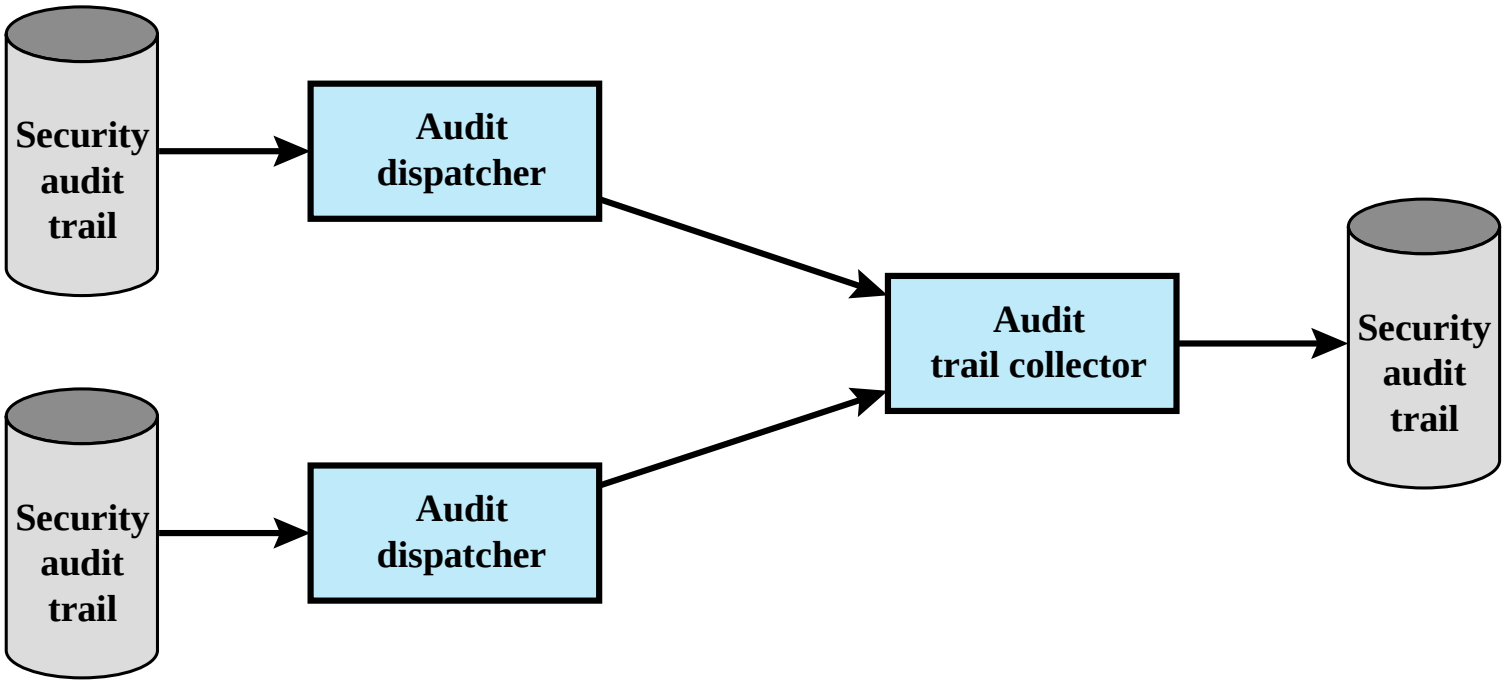


Figure 18.2 Distributed Audit Trail Model (X.816)

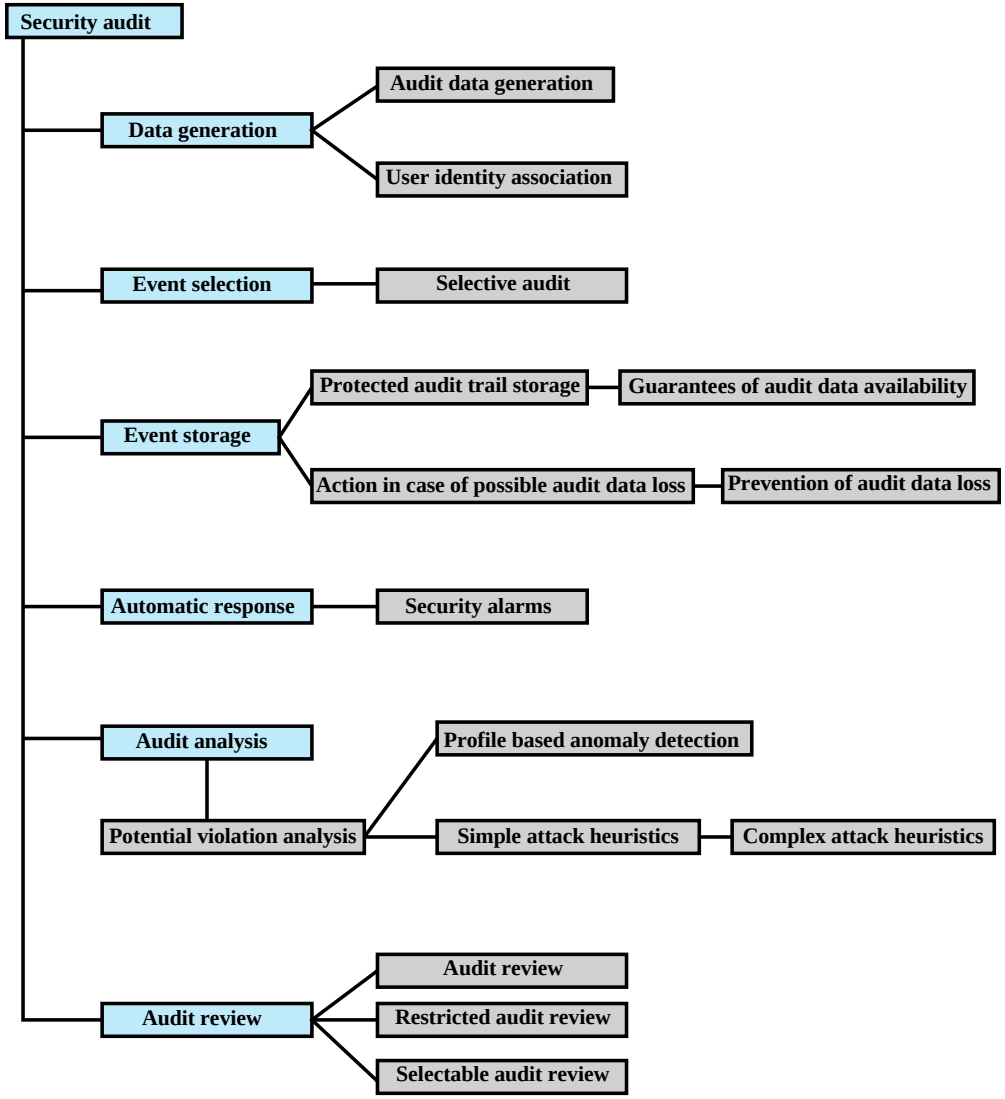


Figure 18.3 Common Critieria Security Audit Class Decomposition

Olay Tanımlama

- Denetime tabi olan olaylar kümesini tanımlamalıdır

Ortak kriter önerir:

- Nesnelerin tanıtımı
- Nesnelerin silinmesi
- Erişim haklarının veya yeteneklerinin dağıtılması veya iptali
- Özne veya nesne güvenlik özniteliklerinde yapılan değişiklikler
- Güvenlik yazılımı tarafından gerçekleştirilen politika kontrolleri
- Politika kontrolünü atlamak için erişim haklarının kullanılması
- Tanımlama ve kimlik doğrulama işlevlerinin kullanımı
- Operatör/kullanıcı tarafından gerçekleştirilen güvenlikle ilgili eylemler
- Çıkarılabilir ortamdan/ortama veri alma/verme

Olay Tespiti

- Olay algılamayı etkinleştirmek için uygulamada ve sistem yazılımında uygun kancalar bulunmalıdır.
- İlgili etkinliği yakalamak için izleme yazılımının sisteme ve uygun yerlere eklenmesi gerekir
- Kurcalamaya veya silmeye karşı dayanıklı güvenli bir depolama sağlama ihtiyacını içeren bir olay kayıt işlevi gereklidir.
- Olay ve denetim izi analizi yazılımı, araçları ve arayüzleri, toplanan verileri analiz etmenin yanı sıra veri eğilimlerini ve anormallikleri araştırmak için kullanılabilir.
- Denetim fonksiyonunun güvenliği için ek bir gereklilik vardır.
- Denetim sisteminin işlevsellik üzerinde minimum etkisi olmalıdır

Uygulama Yönergeleri

Uygun yönetim ile denetim gereklilikleri üzerinde anlaşmaya varılmalıdır

Sistem kullanılabilirliğini etkileyebilecek denetim testleri mesai saatleri dışında çalıştırılmalıdır

Bir referans izi oluşturmak için tüm erişimler izlenmeli ve loglanmalıdır

Teknik denetim testlerinin kapsamı kararlaştırılmalı ve kontrol edilmelidir

Özel veya ek işleme gereksinimleri tanımlanmalı ve kararlaştırılmalıdır

Denetim testleri, yazılım ve verilere salt okunur erişimle sınırlandırılmalıdır

Salt okunur dışında erişime yalnızca sistem dosyalarının yalıtılmış kopyaları için izin verilmelidir

Ne Toplanmalı?

- Denetim yazılımının kullanımı ile ilgili olaylar
- Sistemdeki güvenlik mekanizmaları ile ilgili olaylar
- Çeşitli güvenlik algılama ve önleme mekanizmaları tarafından kullanılmak üzere toplanan olaylar
- Sistem yönetimi ve işletimi ile ilgili olaylar
- İşletim sistemi erişimi
- Seçilen uygulamalar için uygulama erişimi
- Uzaktan erişim

X.816'da Önerilen Denetlenebilir Öğeler

Belirli bir bağlantıyla ilgili güvenlikle ilgili olaylar

- Bağlantı istekleri
- Onaylanan başlantılar
- Bağlantı kesme istekleri
- Onaylanan bağlantı kesmeler
- Bağlantıyla ilgili istatistikler

Güvenlik hizmetlerinin kullanımıyla ilgili güvenlikle ilgili olaylar

- Güvenlik hizmeti talepleri
- Güvenlik mekanizmaları kullanımı
- Güvenlik alarmları

Yönetimle ilgili güvenlikle ilgili olaylar

- Yönetim işlemleri
- Yönetim bildirimleri

Denetlenebilir olayların listesi en azından şunları içermelidir

- Giriş redleri
- Kimlik Doğrula
- Öznitelik değişiklikliği
- nesne oluşturma
- nesne silme
- Nesne değiştirme
- Ayrıcalık kullanımı

Bireysel güvenlik hizmetleri açısından, aşağıdaki güvenlikle ilgili olaylar önemlidir

- Kimlik doğrulama: başarıyı doğrulayın
- Kimlik doğrulama: doğrulama başarısız
- Erişim kontrolü: erişim başarısına karar verin
- Erişim kontrolü: erişimin başarısız olmasına karar verin
- İnkar edilemezlik: mesajın reddedilemez kaynağı
- İnkar edilemezlik: mesajın reddedilemez bir şekilde alındığı
- Reddetmeme: olayın başarısız bir şekilde reddedilmesi
- Reddetmeme: olayın başarılı bir şekilde reddedilmesi
- Bütünlük: kalkan kullanımı
- Bütünlük: kalkansız kullanım
- Dürüstlük: başarıyı doğrulayın
- Bütünlük: doğrulama başarısız
- Gizlilik: gizleme kullanımı
- Gizlilik: açıklama kullanımı
- Denetim: denetim için olay seçin
- Denetim: denetim için olayın seçimini kaldırın
- Denetim: denetim olayı seçim kriterlerini değiştir

ISO 27002'de Önerilen İzleme Alanları

a) kullanıcı kimlikleri
b) sistem faaliyetleri
c) oturum açma ve kapatma gibi önemli olayların tarihleri, saatleri ve ayrıntıları
d) mümkünse cihaz kimliği veya konumu ve sistem tanımlayıcısı
e) başarılı ve reddedilen sistem erişim girişimlerinin kayıtları
f) başarılı ve reddedilen verilerin ve diğer kaynak erişim girişimlerinin kayıtları
g) sistem yapılandırmasındaki değişiklikler
h) ayrıcalıkların kullanımı
i) sistem yardımcı programlarının ve uygulamalarının kullanımı
j) erişilen dosyalar ve erişim türü
k) ağ adresleri ve protokoller
l) erişim kontrol sistemi tarafından verilen alarmlar
m) anti-virüs sistemleri ve izinsiz giriş tespit sistemleri gibi koruma sistemlerinin etkinleştirilmesi ve devre dışı bırakılması
n) uygulamalarda kullanıcılar tarafından gerçekleştirilen işlemlerin kayıtları

```
Jan 27  17:14:04   host1  login: ROOT LOGIN console
Jan 27  17:15:04   host1  shutdown: reboot by root
Jan 27  17:18:38   host1  login: ROOT LOGIN console
Jan 27  17:19:37   host1  reboot: rebooted by root
Jan 28  09:46:53   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
Jan 28  09:47:35   host1  shutdown: reboot by user1
Jan 28  09:53:24   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 12  08:53:22   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 17  08:57:50   host1  date: set by user1
Feb 17  13:22:52   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
```

(a) Sample system log file showing authentication messages

```
Apr 9 11:20:22   host1   AA06370:  from=<user2@host2>, size=3355, class=0
Apr 9 11:20:23   host1   AA06370:  to=<user1@host1>, delay=00:00:02,stat=Sent
Apr 9 11:59:51   host1   AA06436:  from=<user4@host3>, size=1424, class=0
Apr 9 11:59:52   host1   AA06436:  to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 12:43:52   host1   AA06441:  from=<user2@host2>, size=2077, class=0
Apr 9 12:43:53   host1   AA06441:  to=<user1@host1>, delay=00:00:01, stat=Sent
```

(b) Application-level audit record for a mail delivery system

```
rcp       user1   ttyp0    0.02 secs Fri Apr 8 16:02
ls        user1   ttyp0    0.14 secs Fri Apr 8 16:01
clear     user1   ttyp0    0.05 secs Fri Apr 8 16:01
rpcinfo   user1   ttyp0    0.20 secs Fri Apr 8 16:01
nroff     user2   ttyp2    0.75 secs Fri Apr 8 16:00
sh        user2   ttyp2    0.02 secs Fri Apr 8 16:00
mv        user2   ttyp2    0.02 secs Fri Apr 8 16:00
sh        user2   ttyp2    0.03 secs Fri Apr 8 16:00
col       user2   ttyp2    0.09 secs Fri Apr 8 16:00
man       user2   ttyp2    0.14 secs Fri Apr 8 15:57
```

(c) User log showing a chronological list of commands executed by users

Figure 18.4 Examples of Audit Trails

Fiziksel Erişim Denetim İzleri

- Fiziksel erişimi kontrol eden ekipman tarafından üretilir
  - Kartlı anahtar sistemleri, alarm sistemleri
- Analiz ve depolama için merkezi ana bilgisayara gönderilir
- ilgi verileri:
  - Erişim girişiminin tarihi/saati/konumu/kullanıcısı
  - Hem geçerli hem de geçersiz erişim girişimleri
  - Fiziksel erişim ayrıcalıklarını ekleme/değiştirme/silme girişimleri
  - Personele ihlal mesajları gönderebilir

Denetim İzi Verilerini Koruma (RFC 2196-Site Güvenliği El Kitabı,1997)

Ana bilgisayarda dosya okuma /yazma

- Kolay, en az kaynak yoğun, anında erişim
- Davetsiz misafir tarafından saldırıya açık

Bir kez yaz/çok oku aygıtı (CD-ROM veya DVD-ROM)

- Daha güvenli ama daha az kullanışlı
- Kaydedilebilir ortamın sabit kaynağına ihtiyaç var
- Erişim gecikebilir ve hemen kullanılamayabilir

Salt yazılır aygıt (satır yazıcı)

- Kağıt izi sağlar
- Büyük veya ağ bağlantılı sistemlerde ayrıntılı denetim verilerinin yakalanması için pratik değildir
- Kalıcı, hemen kullanılabilir bir log gerektiğinde kullanışlıdır

Hem bütünlüğü hem de gizliliği korumalıdır

- Şifreleme, dijital imzalar, erişim kontrolleri

Loglamanın Uygulanması

- Güvenlik denetim tesisinin temeli, denetim verilerinin ilk elde edilmesidir
- Yazılım, önceden seçilmiş olaylar meydana geldikçe veri toplamayı ve depolamayı tetikleyen kancalar (yakalama noktaları) içermelidir.
- Yazılımın doğasına bağlı
  - İşletim sistemine ve ilgili uygulamalara bağlı olarak değişir

Windows Olay (Event) Logu

- Olay, bazı ilginç olayları tanımlayan bir varlıktır.
  - …… içerir:
    - Sayısal bir tanımlama kodu
    - Bir dizi özellik
    - İsteğe bağlı kullanıcı tarafından sağlanan veriler
- Üç tür olay logu vardır:
  - Sistem: sistemle ilgili uygulamalar ve sürücüler
  - Uygulama: kullanıcı düzeyinde uygulamalar
  - Güvenlik: Windows YSA

Windows Olay Şeması Öğeleri 1/2

İkili veri içeren bir olayın özellik değerleri	Hata ayıklama kanallarındaki hata ayıklama olaylarında kullanılan LavelName Windows yazılım izleme ön işlemcisi (WPP) hata ayıklama izleme alanı
Windows Olay Günlüğü tarafından sağlanan ikili veriler	Bir etkinlik için işlenecek düzey
Oluşturulan etkinliğin yayınlandığı kanal	Bir olay için önem düzeyi
Olay sağlayıcı tarafından sağlanan bir parametre için karmaşık veriler	Hata ayıklama kanallarındaki hata ayıklama olaylarında kullanılan FormattedString WPP hata ayıklama izleme alanı
Hata ayıklama olaylarında kullanılan BileşenAdı WPP hata ayıklama izleme alanı	Bir olay için işlenen olay mesajı
Olayın meydana geldiği bilgisayar	Bir etkinlik için oluşturulacak işlem kodu
İlgili olayları bulmak için kullanılabilen iki adet 128 bitlik değer	Uygulamanın olayı başlattığında gerçekleştirmekte olduğu etkinlik veya etkinlik içindeki bir nokta
Olay verileri işlenirken hataya neden olan olay verisi öğesinin adı	Enstrümantasyon olayını tanımlayan öğeler
Olay sağlayıcı tarafından sağlanan karmaşık veri türünün bir bölümünü oluşturan veriler	Etkinliği yayınlayan etkinlik sağlayıcısı hakkında bilgi
Olay sağlayıcı tarafından sağlanan bir parametre için veriler	Oluşturulan etkinliği yayınlayan etkinlik yayıncısı
Windows yazılım izleme önişlemcisi (WPP) olaylarının özellik değerleri	Bir etkinlik için işlenecek bilgiler

Windows Olay Şeması Öğeleri 2/2

Etkinlik verileri işlenirken bir hata oluştuğunda ortaya çıkan hata kodu	Kullanıcı güvenlik tanımlayıcısı
Sistemdeki bazı ilginç olayları açıklayan yapılandırılmış bir bilgi parçası	Hata ayıklama kanallarında hata ayıklama olaylarında kullanılan SequenceNum WPP hata ayıklama izleme alanı
Olay kimlik numarası	Alt BileşenAdı Hata ayıklama kanallarındaki hata ayıklama olaylarında kullanılan WPP hata ayıklama izleme alanı
Olayın meydana geldiği süreç ve iş parçacığı hakkında bilgi	Olay ortaya çıktığında veya günlük dosyasına kaydedildiğinde sistem tarafından otomatik olarak doldurulan bilgiler
Olay verileri işlenirken hataya neden olan olay için ikili olay verileri	Bir etkinlik için oluşturulacak görev
Süreç ve olayın meydana geldiği iş parçacığı hakkında bilgi	Sembolik değeri olan görev
Hata ayıklama kanallarındaki hata ayıklama olaylarında kullanılan FileLine WPP hata ayıklama izleme alanı	Olayın meydana geldiği zaman hakkında bilgi
FlagsName Hata ayıklama kanallarındaki hata ayıklama olaylarında kullanılan WPP hata ayıklama izleme alanı	Etkinlik bilgilerini ileten herhangi bir geçerli XML içeriğinden oluşabilen sağlayıcı tanımlı kısım
Hata ayıklama kanallarında hata ayıklama olaylarında kullanılan KernelTime WPP hata ayıklama izleme alanı	Hata ayıklamada hata ayıklama olaylarında kullanılan UserTime WPP hata ayıklama izleme alanı
Bir etkinlik için oluşturulacak anahtar kelimeler	Etkinlik sürümü
Etkinlik tarafından kullanılan anahtar kelimeler	

```
Event Type:      Success Audit
Event Source:    Security
Event Category:  (1)
Event ID:        517
Date:            3/6/2006
Time:            2:56:40 PM
User:            NT AUTHORITY\SYSTEM
Computer:        KENT
Description:     The audit log was cleared
Primary User Name:   SYSTEM          Primary Domain:   NT AUTHORITY
Primary Logon ID:    (0x0,0x3F7)     Client User Name: userk
Client Domain:       KENT            Client Logon ID:  (0x0,0x28BFD)
```

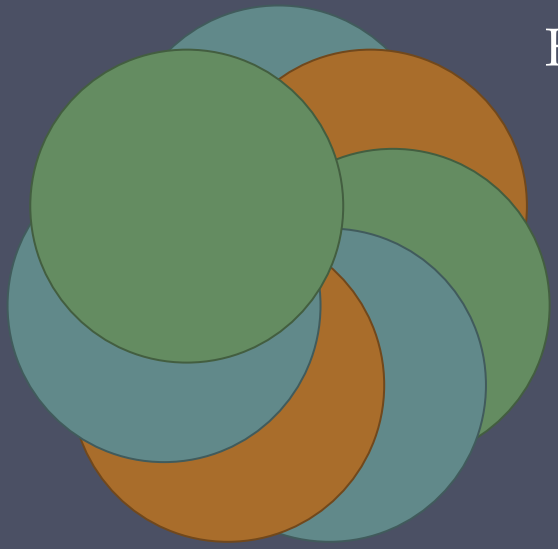
Figure 18.5 Windows System Log Entry Example

Windows Olay Kategorileri

Hesap oturum açma olayları

Ayrıcalık kullanımı

Hesap Yönetimi



Politika değişiklikleri

Dizin hizmeti erişimi

Nesne erişimi

Oturum açma etkinlikleri

UNIX SysLog

- UNIX'in genel amaçlı loglama mekanizması
  - Tüm UNIX / Linux türevlerinde bulunur

Elementleri:

syslog()	logger	/etc/syslog.conf	syslogd
Birkaç standart sistem yardımcı programı tarafından başvurulan ve uygulama programları tarafından kullanılabilen API	Sistem günlüğüne tek satırlık girişler eklemek için kullanılan komut	Sistem günlüğü olaylarının günlüğe kaydedilmesini ve yönlendirilmesini kontrol etmek için kullanılan yapılandırma dosyası	Günlük olaylarını almak/yönlendirmek için Daemon

Syslog Servisi

Temel servisler sunar:

- İlgili olayları yakalamanın bir yolu
- Bir depolama İmkanı
- Sistem logu mesajlarını diğer makinelerden sistem log sunucusu olarak işlev gören merkezi bir makineye iletmek için bir protokol

Ekstra eklenti özellikleri şunlardır:

- Sağlam filtreleme
- Log analizi
- Olay yanıtı
- Alternatif mesaj formatları
- Log dosyası şifreleme
- Veritabanı depolama
- Oran sınırlaması

Syslog Protokolü

- Ana bilgisayarların sistem log sunucularına IP olay bildirim mesajları göndermesine izin veren bir aktarım
  - Çok genel bir mesaj formatı sağlar
  - İşlemlerin ve uygulamaların loga kaydedilen olayları için uygun kuralları kullanmasına izin verir
  - Syslog protokolünün ortak versiyonu, ilk olarak University of California Berkeley Software Distribution (BSD) UNIX/TCP/IP sistem uygulamalarında geliştirilmiştir.
  - BSD syslog formatındaki mesajlar şunlardan oluşur:
  - PRI - tesisler/önem derecesi kodu
  - Başlık – zaman damgası ve ana bilgisayar adı/IP adresi
  - mesaj- programın adı ve içeriği

```
Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from
172.30.128.115 port 21011 ssh2

Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from
10.20.30.108 port 1070 ssh2

Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for
ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!

Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2

Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2

Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

Figure 18.6 Examples of Syslog Messages

UNIX Syslog İmkanları ve Önem Düzeyleri

(a) syslog Facilities

Facility	Message Description (generated by)
kern	System kernel
user	User process
mail	e-mail system
daemon	System daemon, such as `ftpd`
auth	Authorization programs `login`, `su`, and `getty`
Syslogd	Messages generated internally by syslogd
lpr	Printing system
news	UseNet News system
uucp	UUCP subsystem
clock	Clock daemon
ftp	FTP deamon
ntp	NTP subsystem
log audit	Reserved for system use
log alert	Reserved for system use
Local use 0–7	Up to 8 locally defined categories

(b) syslog Severity Levels

Severity	Description
emerg	Most severe messages, such as immediate system shutdown
alert	System conditions requiring immediate attention
crit	Critical system conditions, such as failing hardware or software
err	Other system errors; recoverable
warning	Warning messages; recoverable
notice	unusual situation that merits investigation; a significant event that is typically part of normal day-to-day operation
info	Informational messages
debug	Messages for debugging purposes

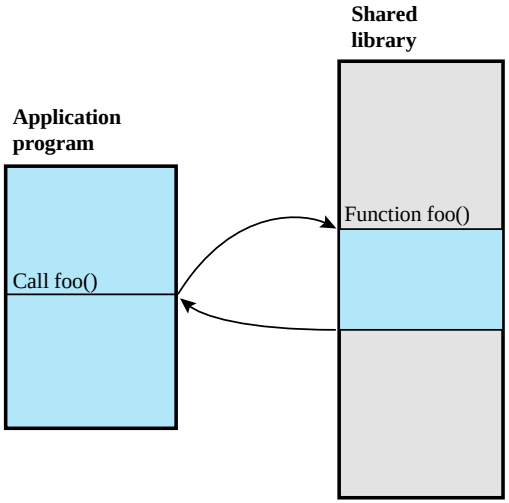
Uygulama Düzeyinde Loglama

- Ayrıcalıklı uygulamalar güvenlik sorunları sunar
  - Sistem/kullanıcı düzeyinde denetim verileri tarafından yakalanmayabilir
  - Bildirilen güvenlik açıklarının büyük bir yüzdesini oluşturur
- Yararlanılan güvenlik açıkları:
  - Girdi verilerinde dinamik kontrollerin olmaması
  - Uygulama mantığındaki hatalar
- Uygulamanın sistem hizmetlerine ve dosya sistemlerine erişiminin ötesindeki davranışını yakalamak için gerekli olabilir
- Denetim verilerini toplamaya yönelik iki yaklaşım:
  - Yerleştirilebilir kitaplıklar
  - Dinamik ikili yeniden yazma

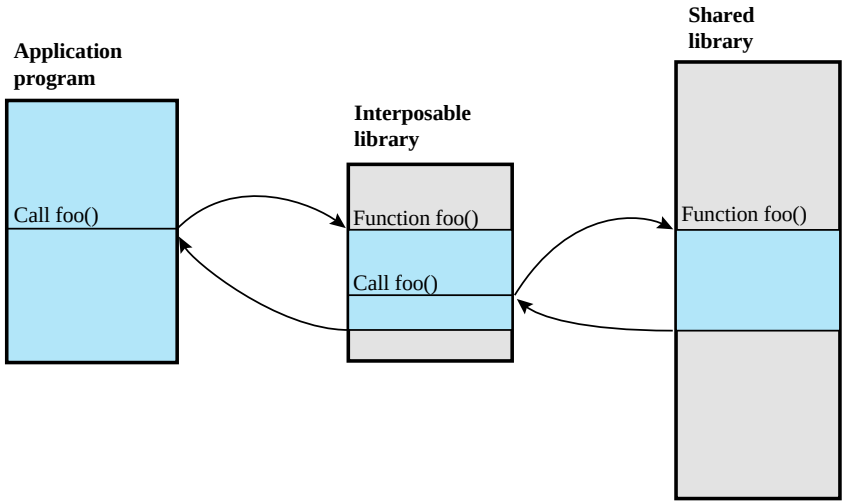
Birleştirilebilir Kütüphaneler

- Sistem kütüphanelerini veya uygulamayı yeniden derlemeye gerek kalmadan denetim verilerinin oluşturulmasına izin verir
- Denetim verileri sistem değiştirilmeden üretilebilir's paylaşılan kitaplıklar veya yürütülebilir dosyanın kaynak koduna erişme ihtiyacı
- UNIX'te dinamik kütüphanelerinin kullanımından faydlanır

- Statik olarak bağlantılı kütüphaneler
  - Bağlantılı kitaplık işlevinin ayrı bir kopyası programa yüklenir'sanal bellek
- Statik olarak bağlantılı paylaşılan kütüphaneler
  - Başvurulan paylaşılan nesne, bağlantı yükleyici tarafından bağlantı zamanında yürütülebilir hedefe dahil edilir
  - Her nesneye sabit bir sanal adres atanır
  - Bağlantı yükleyici, yürütülebilir dosya oluşturulduğunda sanal adreslerini atayarak harici başvurulan nesneleri birbirine bağlar
- Dinamik olarak bağlı paylaşılan kitaplıklar
  - Paylaşılan kitaplık rutinlerine bağlantı, yükleme zamanına kadar ertelenir
  - Yükleme süresinden önce kitaplıkta değişiklik yapılırsa, kitaplığa başvuran herhangi bir program etkilenmez



(a) Normal library call technique



(b) Library call with interposition

Figure 18.7 The Use of an Interposable Library

```
1  /*************************************
2  * Logging the use of certain functions *
3  *************************************/
4  char *strcpy(char *dst, const char *src) {
5     char *(*fptr)(char *,const char *);    /* pointer to the real function */
6     char *retval;                          /* the return value of the call */
7
8     AUDIT_CALL_START;
9
10    AUDIT LOOKUP COMMAND(char *(*)(char *,const char *),"strcpy",fptr,NULL);
11
12    AUDIT_USAGE_WARNING("strcpy");
13
14    retval=((*fptr)(dst,src));
15
16    return(retval);
17 }
```

(a) Function definition (items in all caps represent macros defined elsewhere)

```
1 #define AUDIT_LOOKUP_COMMAND(t,n,p,e)
2    p=(t)dlsym(RTLD NEXT,n);
3    if (p==NULL) {
4        perror("looking up command");
5        syslog(LOG_INFO,"could not find %s in library: %m",n);
6        return(e);
7    }
```

(b) Macro used in function

Figure 18.8 Example of Function in the Interposed Library

Dinamik Binary Yeniden Yazma

- Hem statik hem de dinamik olarak bağlantılı programlarla kullanılabilir
- derleme sonrası yürütülebilir dosyaların ikili kodunu doğrudan değiştiren teknik
  - Değişiklik, yükleme sırasında yapılır ve bir programın yalnızca bellek görüntüsünü değiştirir.
  - Uygulama ikili dosyasının yeniden derlenmesini gerektirmez
- Linux'ta iki modül kullanılarak uygulanmıştır:
  - Yüklenebilir çekirdek modülü
  - İzleme cini (daemon)
- Yüklenebilir modüller
  - Talep üzerine otomatik olarak yüklenebilir ve boşaltılabilir

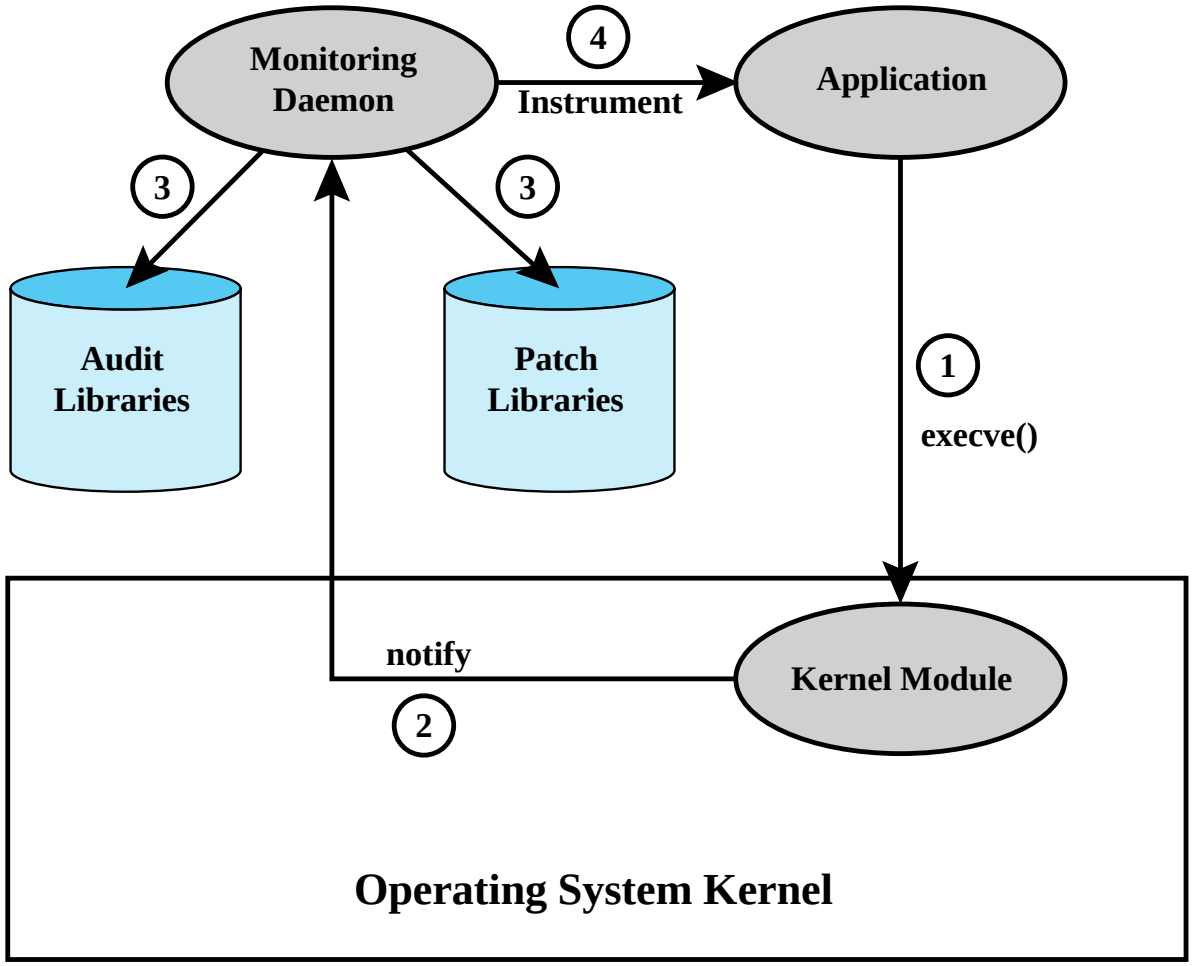


Figure 18.9 Runtime Environment for Application Auditing

Denetim İzi Analizi

- Analiz programları ve prosedürleri büyük ölçüde değişir
- Log girişlerinin bağlamını anlamalıdır
  - İlgili bilgiler, aynı loglardaki diğer girişlerde, diğer loglarda ve log olmayan kaynaklarda bulunabilir.
- Denetim dosyası formatları, düz metin ve kodların karışımını içerir
  - Manuel/otomatik olarak deşifre edilmelidir
- Temel durumu anlamak için girişleri ideal olarak düzenli olarak gözden geçirin

Denetim İzi Analizi Türleri

Denetim izleri birçok şekilde kullanılabilir	Olasılıklar şunları içerir:

• Bu kısmen ne zaman yapıldığına bağlıdır	• Bir olaydan sonra denetim izi incelemesi
	  • Nedeni teşhis etmek ve düzeltmek için olay tarafından tetiklenir
	  • Belirli bir olayla ilgili denetim kaydı girişlerine odaklanır
	• Denetim izi verilerinin periyodik olarak gözden geçirilmesi
	  • Sorunları ve davranışı belirlemek için toplu verileri incelenir
	• Gerçek zamanlı denetim analizi
	  • İzinsiz giriş algılama işlevinin bir parçası

Denetimin İncelenmesi

- Denetim gözden geçirme özelliği, yöneticiye seçilen denetim kayıtlarından bilgi sağlar
  - Bir veya daha fazla kullanıcının eylemleri
  - Belirli bir nesne veya kaynak üzerindeki eylemler
  - Denetlenen istisnaların tümü veya belirli bir grubu
  - Belirli bir sistem/güvenlik özniteliğine ilişkin eylemler
- Zamana/kaynağa/frekansa göre filtrelenebilir
- Sistem etkinliği temeli sağlamak için kullanılır
- Güvenlikle ilgili faaliyet düzeyi

Veri Analizinde Yaklaşımlar

Basit uyarı

- İlginç türde bir olayın gerçekleştiğini belirtir

Temel çizgi

- Normal ve olağan dışı olayları/kalıpları tanımlar
- Değişiklikleri tespit etmek için yeni verilerle karşılaştırır
- Eşikleme, belirli bir temel değeri aşan verilerin tanımlanmasıdır

Çerçeveleme

- Belirli bir parametre kümesi içindeki olayların algılanması

Korelasyon

- Olaylar arasındaki ilişkileri arar

SIEM Sistemleri

- Yazılım, syslog'a benzer, ancak ondan çok daha karmaşık, merkezi bir günlük kaydı yazılım paketidir.
- Merkezi, tek tip bir denetim izi depolama tesisi ve bir dizi denetim verisi analiz programı sağlayın
- İki genel yapılandırma yaklaşımı vardır:
  - aracısız
    - SIEM sunucusu, günlük üreten ana bilgisayarlardan, bu ana bilgisayarlara herhangi bir özel yazılım yüklenmesine gerek kalmadan veri alır.
  - aracı tabanlı
    - Belirli bir günlük türü için olay filtreleme ve toplama ve günlük normalleştirmesi yapmak ve ardından normalleştirilmiş günlük verilerini genellikle gerçek zamanlı veya neredeyse gerçek zamanlı olarak bir SIEM sunucusuna iletmek için günlük üreten ana bilgisayara bir ajan programı kurulur. analiz ve depolama için temel

SIEM Yazılımı