

ÇOK KATMANLI DEĞİŞEBİLİR SALDIRI TESPİT SİSTEMLERİ (MAIDS)

1-) GİRİŞ

Jim Anderson saldırı tespit konusunu 1980`de ortaya atmıştı.Ona göre bir saldırı, izin olmadan:

- Bilgiye ulaşım
- Bilgiyi değiştirme
- Sistemi kullanılmaz veya güvenilir hale getirme

İşlemleri idi.**STS`ler**, yani **saldırı tespit sistemleri**, ise bu durumlarda ortaya çıkarak kimin sisteme ne zaman bağlandığını ve neler olduğunu belirlemek amacıyla düzenlenmiş yazılımlardır.

1.1) Saldırganlar kimlerdir?

- Dış saldırganlar (Sistemi kullanmaya izni olmayan kişiler)
- İç saldırganlar (Sistemi kullanmaya izni olan fakat belli bir bilgiye, yazılıma veya kaynağa ulaşmaya izni olmayan kişiler. Bu gurup maskelenmiş (başka bir kişinin kullanıcı ismi ve şifresini kullanan kişiler) ve gizli (normal kontrollerden kaçarak kendini gizleyen) kullanıcıları da içermektedir.
- Sistemi kullanmaya ve bilgiye erişmeye hakkı olup, verilen izin haklarını kullanarak diğer kaynaklara erişmeye çalışan kullanıcılar.

2.2) Saldırı Tespit Sistemleri sınıflandırılması

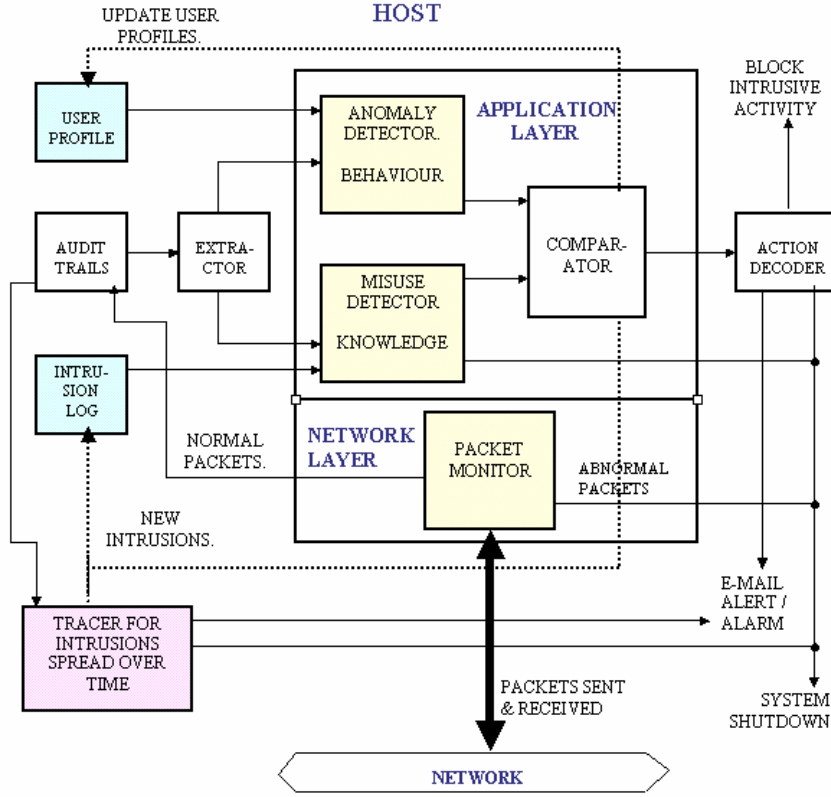
Simdi de STS`leri (saldırı tespit sistemi) sınıflamaya calisalim:

a) Tespit metoduna göre:

- Değişiklik tespiti: Bu tur STS`leri kullanıcı davranışları olarak adlandırılan belirli bir modeli örnek alır.Bu örnek dışındaki davranışlar anormal olarak Kabul edilir.
- Yanlış kullanım tespiti: Bu STS`leri daha önce belirlenmiş, imza adi verilen ve saldırıları tespit etmek için hazırlanmış olan örnekler ile çalışırlar.

b) **Hedef sistemin tipine göre:**

- Sistem bazli: Bu tur STS`ler tek bir sistem uzerindeki bilgileri inceler
- Ag bazli But tur STS`ler tum ag trafiginin inceler.



Resim 1: Sistem mimarisi

Yesil : Genetik algoritma kullanir
Sari: Ana bileşken
Pembe : Bilgi araştırma kullanir

2-) MAIDS Mimarisi

2.1) Fonksiyonel Parçalar

STS`lerin fonksiyonel parçaları şunlardır:

Paket monitörü

Network katmanında çalışır. Alınan ve gönderilen paketleri inceler. Bu paketlerde bulunan belli bit alanlarının bulunup bulunmamasına göre bir saldırı olup olmadığı belirleyebilirler. Kontrol edilen bu alanlar şunları içerir:

- Değişik kaynak IP adresleri

- TCP kaynak port`u ve hedef port`u 21
- Servis tipi 0
- İp tanımlama numarası 39426
- SYN ve FIN flag`leri tanımlanmış
- TCP pencere boyutu 1028 vs.

Ayrıştırıcı

Ayrıştırıcı elde edilen bilgiyi yanlış kullanım veya anormallik ajanları tarafından analiz edilebilmeleri için gruplara ayırır. Akilli bir ajan olarak gelen bilgiler içinden ise yarayacak olanları ayırıp gerekli ajanlara, gerekirse gelen bilgiyi düzenleyerek yollar.

Amaç dışı kullanım bulucu

Bu bulucu birbirinden ayrı şekilde çalışan ve izleyici olarak adlandırılan işlemlerin bir toplamı olarak adlandırılabilir ve şunları içerir:

Sistem izleyici su sistem seviyesi parametrelerinin işleyişini kontrol eder:

İşlemci kullanımı
Bellek swap alanı
I/O kullanımı vs.

İşlem izleyici işlem seviyesi parametrelerini izler:

İşlem tip ve numaraları
İşlem süresi
İşlemin o andaki durumu

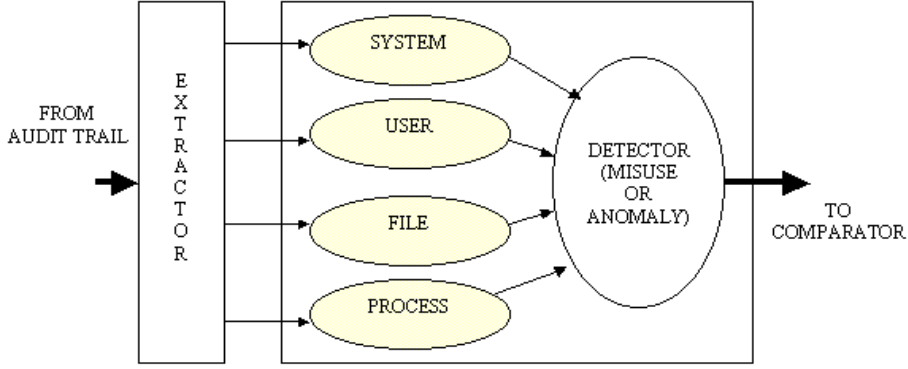
Dosya izleyici dosya seviyesi parametrelerini izler:

Dosya sayıları
Dosya sahibinin kullanıcı numarası
Dosya sahibinin grup numarası

Kullanıcı izleyici kullanıcı seviyesi parametrelerini izler:

Kullanım gün ve zamanı
Sistem giriş zamanı
Özel komutlar

Bu izleyiciler kendi parametrelerini (ayrıştırıcı tarafından onlara gönderilen bilgiyi) belli saldırı senaryolarına göre hazırlanmış olan parametreler ile karşılaştırırlar. Eğer bir eşlik söz konusu olursa bunun bir saldırı olduğu kesinleşir. Eğer benzerlik yok ise bütün bu değerler birleştirilerek, o andaki işlemin nasıl kesileceğini belirten bir "k" değeri ortaya çıkarılır.



Resim 2: Ajan bazlı mimari.

Anomali Bulucu

Yanlış kullanım bulucusu gibi bu da birbirinden ayrı işleyen izleyicilerin oluşturduğu bir gruptur. Bu işlemlerin asıl amacı belli bir işlemin normal davranışa ne kadar yakın olduğunun belirlenmesidir. Eğitim dönemi sırasında her kullanıcı için hazırlanan belli bir kullanıcı profili bulunmaktadır. Bu profil her kullanıcı için en fazla olabilecek değerleri içerir. O anda yapılan işlemler bu profiller ile karşılaştırıldığında ortaya, kullanıcının normal davranışlarına ne kadar yakın işlemler yaptığını ortaya koyan bir "b" değeri çıkmaktadır.

Karşılaştırıcı

Karşılaştırıcı anomali bulucusundan gelen girdileri yani "b" ve "k" yi karşılaştırır. Bunun sonucuna göre o andaki işlemi, güçlü normal, zayıf normal, zayıf saldırı ve güçlü saldırı olarak adlandırılan dört durumdan birisine dahil edip faaliyet çözücüne gönderir.

Faaliyet çözücü

Faaliyet çözücü gelen girdiye göre aşağıda belirtilen çıktılarından birisini verir:

- . Sistem yöneticisine bir uyarı e-postası veya uyarı göndermek
- . Sistemi kapatmak
- . Saldırgan faaliyeti bloke edip sistem yöneticisini haberdar etmek.

Geniş zamana yayılı saldırı takip edici

Bazı saldırı senaryoları bir saat veya birkaç gün gibi geniş zamana yayılı olabilir. Bu tür bir durumda yapılan faaliyetler teker teker bakıldığında saldırgan içerikli değil fakat bir araya getirildiğinde saldırgan içerikli olabilirler. Bu parça bu tür saldırılar ile ilgilidir.

2.2) Günlükler

Hesap izleri

Hesap izleri işletim sistemi tarafından, sistemin o andaki durumunu belirten bilgilerden oluşur. Normal paketler paket izleyici tarafından yakalanan bilgiler hesap izlerini güncellemek için kullanılır. Hesap izi günlükleri eski ve yeni sistem faaliyetleri hakkında bilgi içerir.

Saldırı Günlüğü

İki tur günlükten oluşur:

Tek saldırı günlüğü: Belirlenen tek saldırı faaliyeti günlüğüdür. Her yeni saldırı tespitinde güncellenir.

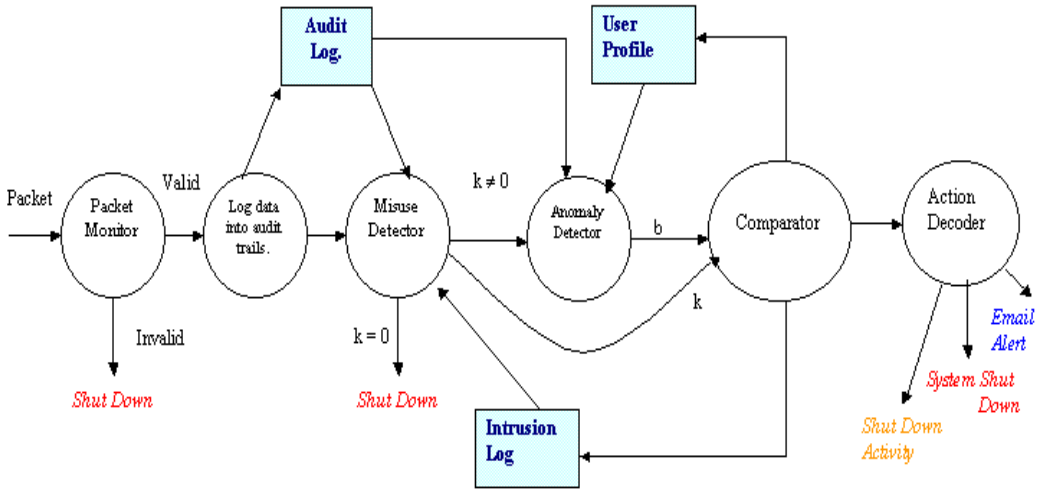
Sürekli saldırı günlüğü: Belirlenen sürekli saldırı günlüğüdür. Eğitim döneminde hazırlanır ve her yeni saldırı tespitinde güncellenir.

Kullanıcı profili.

Kullanıcı tarafından yapılan faaliyetlerin belirlenmesi mümkündür. Bu tür belirleme işlemi sonucunda ortaya çıkan bilgiye kullanıcı profili adı verilir. Bu kullanıcının normal davranış ve izin verilebilen faaliyetlerini içerir. Bu kişinin kendi faaliyetlerini üzerine hazırlanması yanında grup faaliyetlerini de baz alarak hazırlanabilir. Kişisel faaliyetler zamanla değişim geçireceğine göre kullanıcı profilinin zaman içinde bu değişikliklere göre güncellenmesi gerekmektedir. Burada bahsedeceğimiz Genetik Algoritma devamlı olarak kullanıcı profillerini güncelleyecektir.

2.3) Bilgi Akış Diyagramı

Sistemin fonksiyonlarını nasıl gerçekleştirdiğini belirtir.



Resim 3 : Bilgi akış diyagramı

3) IDS Algoritması

Adım 1: Basla

Adım 2: Paket monitoru ağ üzerinde alınan ve ağa gönderilen paketlerin üzerindeki kontrol alanları kontrol eder. Eğer paketler anormal bulunursa IDS sistemi kapatarak cevap verir. Eğer paketler normal ise 3. adıma geçilir.

Adım 3: Normal paketler hesap izleri günlüklerine kaydedilir.

Adım 4: Ayırıştırıcı bunları kategoriler ve bu bilgileri diğer izleyicilere gönderir

Adım 5: Amac dışı kullanım bulucusu tek saldırı günlüğünde bulunan senaryolara göre gelen bilgileri kontrol eder. Eğer bir benzerlik bulunursa bu bir saldırıdır ve STS sistemi kapatır. Eğer benzerlik yok ise adım 6 ya geçilir.

Adım 6: Amac dışı kullanım bulucusu, bir faaliyetin saldırıya ne kadar yakın olduğunu belirten “k” değerini bulur ve bu değer karşılaştırmaya gönderilir.

‘k’ değerinin bulunması

Tek saldırı günlüğünden alınan her j saldırı için “k” değeri bulunur. Saldırıları genetik algoritma ile seçilirler. n değerinin tek saldırı günlüğünde bulunan tüm parametreler toplamı olduğunu varsayalım.

Her parametre için saldırı için p_i değeri günlükten okunacaktır. Parametrenin o anki değeri ise hesap izleri günlüğünden alınır c_i olarak adlandırılır.

Verilen her parametre için sapma oranı

$$\delta_{ji} = |p_i - c_i|$$

j^{th} saldırısı için toplam sapma

$$\delta_j = \sum \delta_{ji}$$

j^{th} saldırısında k'nin değeri

$$k_j = \delta_j / n$$

k'nin değeri: $k = \min(k_j)$

Bunun yanında j saldırısı aşağıdaki şartları yerine getirmelidir:

Tüm parametreler g_i olarak, yani önem sırasına göre gruplanmış olarak hazırlanmalı

N_i numarasının g_i grubundaki parametre sayısı olduğunu farzedelim.

X_i ve Y_i değerleri sistem yöneticisi tarafından hazırlanır ve saldırı sırasında incelenmesi gereken en az yanılma payını belirtmeli.

Herhangi iki saldırı, ayrı parametre sayılarına sahip olup, aynı yanılma payını verebilir $\delta_{ji} \leq 2.0$. En iyi tahmini bulabilmek için parametreleri önem sıralarına göre sıralayıp $\delta_{ji} \leq 2.0$ değeri olması gereken en az parametre sayısını belirleyebiliriz.

Adim 7: Anomali bulucusu, o andaki faaliyetin, kullanıcı profilinde belirtilen normal davranışa ne kadar yakın olduğunu belirten “b” değerini bulur. Bu değer karşılaştırmaya verilir.

“b” değerinin bulunması

Değişik kategorilerde bulunan parametreler (sistem, kullanıcı, işlem ve dosya), parametrenin önemini belirten bir ağırlık yani w_i değeri alırlar. Bu parametrelerden her biri için sınır, t_i değeri belirlenir. Bu değer her kullanıcı için ayrı olacak ve her kullanıcının o parametre için izin verilen parametre değerini belirtmektedir.

Parametrenin o anki değeri hesap izlerinin günlükünden alınır ve c_i olarak adlandırılır:

$w_i \cdot t_i$ = parametre için güvenli değer,

$w_i \cdot c_i$ = parametrenin şu andaki değeri

b_j = Kategoriyeye dahil parametreler için gözetleyici tarafından verilen değer $j=1,2,3,4$. (4 kategori parametre için)

$b_j = \sum (w_i \cdot t_i \cdot w_i \cdot c_i) / n_j$

n_j = o kategorideki parametrelerin sayısı.

Net değeri $b_j = \sum (w_i \cdot t_i - w_i \cdot c_i) / n_j$

$b_{max} = \sum b_{jmax} / 4$ te $b_{jmax} = \sum w_i \cdot t_i / n_j$ olarak çıkar.

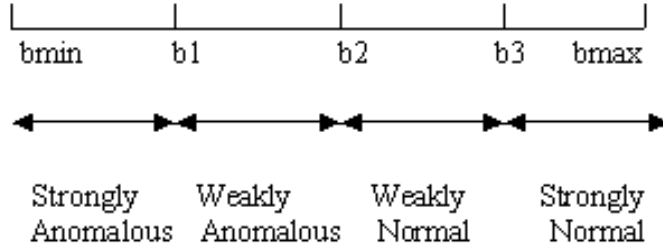
$0 \leq b \leq b_{max}$, artan b değerleri sistemin daha normal hale geldiğinin işaretidir. $b=0$ en güvenli ve $b=b_{max}$ hiçbir sistem kullanımı olmadığını belirtir.

Adim 8: Karşılaştırmacı, o andaki faaliyet durumunu belirtilen dört ayrı durumdan birisine dahil etmek üzere “b” ve “k” değerlerini karşılaştırır. Karşılaştırmacı çıktısı faaliyete geçirilerek gönderilir.

Karşılaştırmacı nasıl çalışır?

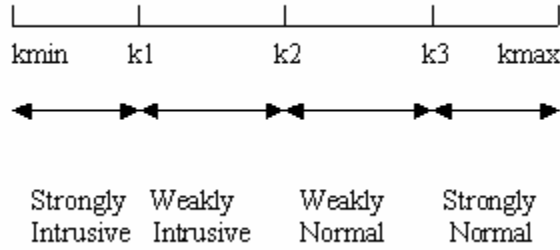
$b_{min} \leq b \leq b_{max}$, $k_{min} \leq k \leq k_{max}$ olduğunu farzedelim. $(b_{max}-b_{min})$ & $(k_{max}-k_{min})$ arasındaki dizi dört bölüme ayrılmıştır. Bu bölümler yapılan faaliyetin doğasını belirtmektedirler. Diğer bir deyişle eğer bir dizinin içinde değişik faaliyetlerin değerleri bulunuyorsa, değişik faaliyetlerin doğası aynı olarak kabul edilebilir.

örnek: $b_{max}-b_{min}$ ’in 4 bölüme ayrıldığını farz edin:



Resim 4: "b" nin dağılım tablosu

Bu bölümlerin genişlikleri değişebilir.Örneğin "en güçlü normal" bölümünün muhtemelen en ufak genişliği olacaktır.Buna ek olarak yeni başlatılan bir işlem bir bölümden diğerine geçebilir. Bunun gibi kmax-kmin`de dört bölüme ayrılmıştır:



Resim 5: "k" nin dağılım tablosu

Bunun sonunda karşılaştırmacı, o andaki faaliyeti aşağıdaki şekilde sınıflayacağı, önceden hazırlanmış bir faaliyet durum tablosuna sahip olur:
 Güçlü saldırı (SI)
 Zayıf saldırı(WI)
 zayıf normal (WN)
 güçlü normal(SN)

Sistem yöneticisine sistemi yönetme seçeneğini iki şekilde verebiliriz: Az risk taşıyan işlemlere izin vermesini sağlayan az risk kipi ve hiçbir riskli faaliyete izin vermeyen risksiz kipi.

B	k	Low Risk	No Risk
1	1	SI	SI
1	2	SI	SI
1	3	SI	WI
1	4	SI	WI
2	1	SI	SI
2	2	WI	WI
2	3	WI	WN
2	4	WN	WN
3	1	SI	SI
3	2	WI	WN
3	3	WN	SN
3	4	SN	SN
4	1	SI	SI
4	2	WI	WN
4	3	SN	SN
4	4	SN	SN

Adim 9: Faaliyet çözücü karşılaştırıcıdan gelen çıktıyı çözer ve aşağıdaki cevaplardan birisini verir:

State of Activity.	Response.
SI	A
WI	B
WN	C
SN	D

- A) Faaliyeti durdur: Faaliyeti durdurup sistem yöneticisine haber verir.
- B) uyarı: Faaliyeti durdurmaz fakat sistem yöneticisini uyarır
- C) Tampon(Buffer): Faaliyeti tampon bölgeye alıp önceden belirlenmiş bir süre izler. Bu süre sonunda eğer faaliyette hiçbir değişiklik yoksa sistem yöneticisini uyarır. eğer değişiklik var ise faaliyet tampon bölgeden çıkartılıp gerekli işlem yapılır.
- D) Gecis: Faaliyete dokunmaz ve akisina izin verir.

Adim 10: Adim 2 ye geri don

4) Genetik Algoritma Kullanimi (GA)

Genetik algoritmalar (GA), dogal biyolojik evrimi taklit eden, genel amacli arama methodlari sinifini temsil eder. Genetik algoritmalar, en iyi coumu bulabilmek icin en guclunun yasamasi kuralina gore calisan bir yontem kullanirlar (kromozomlar). Genel olarak bir GA `in duzgun calisabilmesi icin asagidaki uc icerik tanimlanmalidir:

- 1-) Kromozom`un sifrenlenmesi problem alanini belirtir
- 2-) Kromozomun uygunluk olcumu cozumlerin kalitesini belirtir
- 3-)Genetik yoneticiler uye cozumlerini yonetmek icin kullanılan degisim yoneticileridir.

Nufusun her uyesinin uygunluk derecesi probleme gore herbirinin ne kadar iyi davrandigini olcen degisik fonksyonu ile belirlenir.Daha iyi performans sahip uyeler odullendirilirken daha az performans sahip olanlar cezalandirilir veya atilir.Rastgele bir nufus ile baslarsak genetic algoritma o anda bulunan nufustaki bilgiyi isler ve yeni uyeleri genetic yoneticiler sayesinde yenilerini olusturarak arastirir.Bu secmeli besleme yontemi sonucunda yuksek olasiliga sahip bir sonuc ortaya cikir.Birkac cesit genetic yoneticisi gelistirilmis olmasina ragme, yeni kromozomlar uretmek icin en cok kullanılan degisim ve gecis yoneticileridir.

Geçis yoneticisi bir çift kromozom arasında bilgi degisimi yapar.Degisim yoneticisi ise belirlenen kromozomda, arastirilmamis bolumu aramak icin , bir veya birkac gende degisiklik yapar.

Sistemimizde GA `yi uc yerde kullaniyoruz:

4.1) Kullanici profillerini guncellemek

Gereklilik:

Kullanici profilleri, kullanici faaliyetlerine gore egitim periyodunda belirlenmektedir.Bu aktiviteler zamanla degisebilir ve bu yuzden bir saldiri olarak algılanmamalidir.Iste bu yuzden burada GA kullanmaktayiz.

Genetik terim ve yoneticisi (operatör) tanımlamaları

Kromozom

Parametrenin maksimum deęerini binary (ikili) şekilde belirten (0,1) dizidir.Her parametre 4-bit ikili dizi olarak temsil edilmektedir.

Threshold Value	Chromosome Encoding
0.0	0000
0.1	0001
0.2	0010
:	:
:	:
1.0	1010

Dizideki özel parametrelerin pozisyonu düzenlenmiştir.
örnek: 3 parametreye bakalım

İşlemci kullanımı, i/o kullanımı ve işlem sayısı ve bunların maksimum değerleri 0.5,0.6 ve 0.7 olsun.Buna göre kromozom dizisi şöyle olacaktır:
0101 0110 0111

İlk nüfus

Ayrıştırıcı tarafından tampon bölgeye alınan hesap izi kayıtlarının kodlanmış halidir.

Yöneticiler (operatör`ler)

Güncellenmiş davranışları en iyi şekilde almak için kullanılacak olan geçiş ve değişim yöneticileridir.

Uygunluk Değerlendirmesi

kullanıcı profili kromozomu ve o anki faaliyet kromozomları arasında bir karşılaştırma tutulmaktadır.

$$\delta = \sum [w * |belirlenmiş . su andaki|]$$

W= ağırlık Parametre önemliliği.değerleri sistem yöneticisi tarafından belirlenebilir.

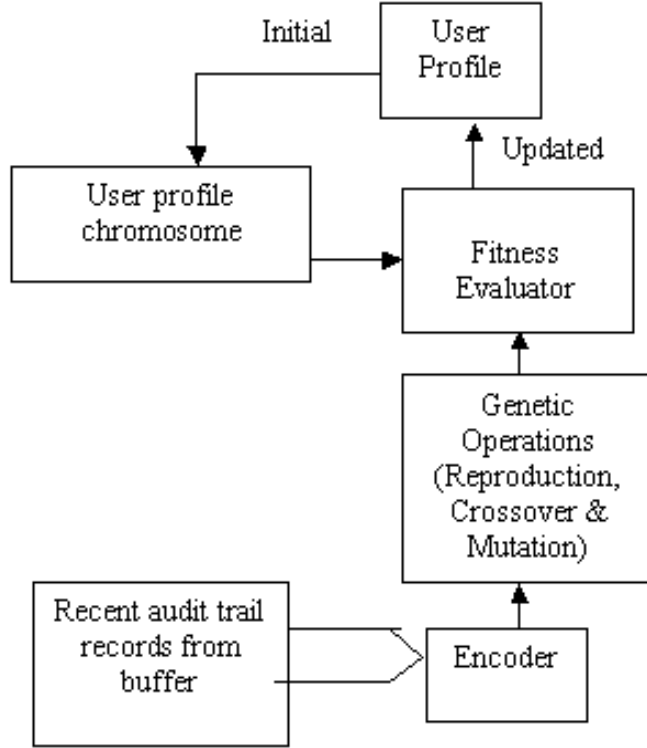
Uygunluk değerlendirme fonksiyonu = (formül)

δ `un değeri azaldıkça profili güncellemeye uygunluk o kadar artar.

Dizayn:

Adım 1: Ayrıştırıcı hesap takip bilgisini bir kullanıcı oturumundaki geçici tampon bölgeye alır.Bu tampon bölgenin içeriği o anki faaliyet`in bir çeşit olcusudur ve burada daha önceden belirlenmiş bir süre tutulurlar.eğer bu süre içinde hiçbir saldırı bulunmazsa bu bilgi o anki nüfusu belirlemek için kullanılır.eğer saldırı tespit edilirse tampon bölgedeki bilgi saldırı günlüğünü güncellemek için kullanılır.

Adım 2: Tampon bölge bilgisi kromozom formundaki ilk nüfusu oluşturmak için kodlanır.



Resim 6: kullanıcı profilinin güncellenmesi için GA bileşeni

Adım 3 : Geçiş ve değişim yöneticileri yardımıyla, muhtemel kullanıcı davranışını belirtecek olan kromozomlar oluşturulur.

Adım 4: Bu kromozom seti , kromozomların,kullanıcı profilini güncellenmek için kullanılacak en uygun kromozomu belirlemek için belirlenmiş kullanıcı profili ile karşılaştırıldığı uygunluk değerlendirici`ye verilir.

Adım5: Bu çıktı kullanıcı profilini güncellemek için kullanılır.

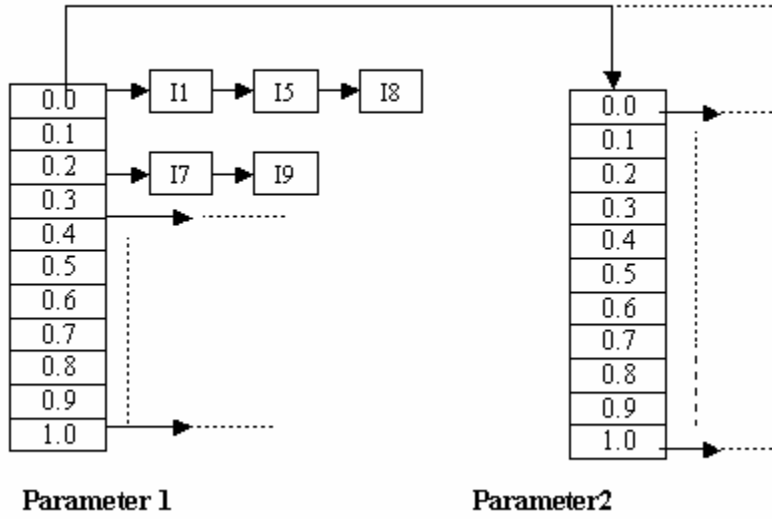
4.2) Tek saldırı günlüğünün aranması

Gereklilik:

Tek saldırı günlüğünün büyüklüğü arttıkça her saldırı için bulunması gereken k değerinin araştırılması da daha uzun süre almaya başlar.Bunu önlemek için daha önceden kısaltılmış bir dizi alınır.Bu işlem iki bölümden oluşur:

Azaltma işlemi:

Adım 1:Tek saldırı günlüğü her parametre için bir tane olmak üzere hesaba dayalı adresleme (hash) tablolarından oluşur.Bu tablolardaki her bolum 11 mümkün parametre değeri içerir.Bu bölümler her bolum için temsil edilen parametreye denk gelen saldırı senaryolarını gösterir.



Resim 7: Hesaba dayalı adresleme tablosu organizasyonu

O anki faaliyet parametre değerlerine göre hesaplama işlemi her parametre için yapılar, buna uygun saldırı listesi çıkartılır.

eğer listeler içinde belli bir saldırıyı bulunursa bu harika saldırı ($k=0$) olarak adlandırılır. eğer hesaplama sonunda elde edilen saldırı sayıları çok yüksek ise, nüfusu azaltmak için sıklık kontrolü gibi yöntemler ile optimizasyon yapılır.

Adım 2: Bu bölüm genetik algoritma kullanır

Genetik terim ve yönetici tanımlamaları

Kromozom

Parametrenin maksimum değerini binary (ikili) şekilde belirten (0,1) dizidir. Her parametre 4-bit ikili dizi olarak temsil edilmektedir.

İlk nüfus

Adım1 de oluşturulan saldırı listelerinin kodlanmış şeklidir

Yöneticiler

O anki faaliyeti yanından en yakın saldırıyı bulabilmek için kullanılan geçiş ve değişim yöneticileri

Uygunluk Değerlendirmesi:

Saldırı kromozomları ve o anki faaliyet kromozomları arasında bir karşılaştırma tablosu tutulur.

Uygunluk değerlendirme

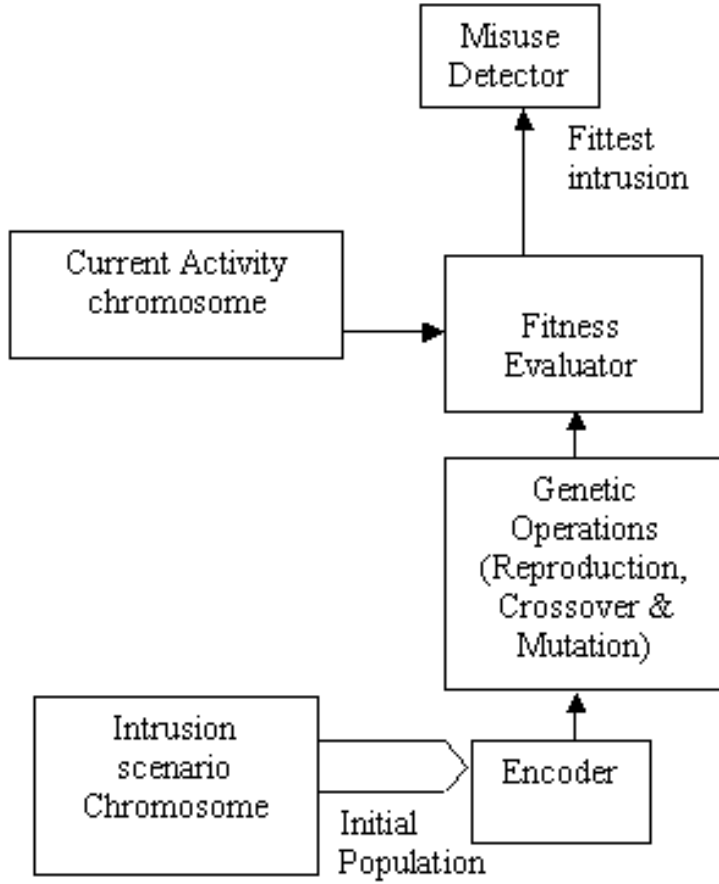
$$= \delta = \sum | \text{saldiri} . \text{su andaki} |$$

δ degeri azaldikca "k" degerlendirilmesinde kullanilma olasiligi artar

Dizayn:

Adim 1: Kromozom halinde olan nugusu olusturmak icin saldiri listesindeki saldirilar kodlanir

Adim 2: Bazi kromozomlarin yeniden olusturulabilmesi icin, gecis ve degisim yoneticileri yardimiyla, bir dizi kromozom olusturulur. Bu kromozomlar o anki faaliyete yakinligi belirtir.



Resim 8: saldiri günlüğünün araştırılması için GA bileşeni

Adim 3: "k" deęerinin deęerlendirilmesi için en uygun olanların belirlenmesi için alınan dizi o anki faaliyet kromozomları ile karşılaştırılır.

Adim 4: çıktı amaç dışı kullanım bulucusuna verilir.

4.3) Kullanıcı profillerinin oluşturulması:

Kullanıcı profilleri, bu süre içinde hiçbir saldırı olmadığı farz edilen eğitim süresinde geliştirilir. Eğitim süresinde kullanıcının faaliyetleri kullanıcı profilini oluşturmaya odaklanmıştır. Bu süre içindeki kullanıcı faaliyetleri, kromozom halindeki nüfusu oluşturmak için kodlanır. Bu kromozomlar, daha sonra kullanıcı profilini temsil edecek olan tek kromozomu bulabilmek için, kendi aralarında geçiş ve değişim yöneticileri yardımıyla tekrar oluşturulurlar.

5) Bilgi araştırması

Bilgi araştırması genel olarak büyük kapasitedeki bilgi içinden gerekli olan modellerin çıkarılması işlemidir. Bu konuda elde edilen gelişmeler, istatistikler çıkartan, öğrenebilen ve veritabanları gibi birçok değişik algoritmayı da beraberinde getirmiştir.

Sınıflama

Bir bilgiyi daha önceden belirlenmiş sınıflardan birine dahil eder.
Bağlantı analizi: Veritabanı içindeki bölümler arasında bağlantıları bulur.
Sıra analizi: Dizisel yolları belirler

Dizayn

Birleştirme kuralları:

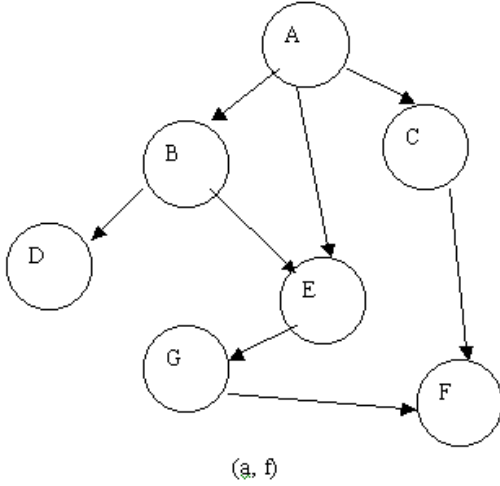
İki olay arasındaki bağlantı bir olayın olma olasılığını belirtir. Bu bağlantı arasındaki sıklıkta ayrıca depolanır.
örnek: Y olayı gerçekleştiğinde X olayının gerçekleşme olasılığı şöyle belirtilir:

$$Y \Rightarrow X(a, f)$$

A= Birleşim parametresi

B=Y`yi takip eden X`in oluşma sıklığı

Saldırı senaryoları, devamlı saldırı günlüklerinde, eğitim süresi sırasında ağaç diziler şeklinde depolanır.



Resim 9: saldırı olayları ağacı

Saldırı senaryolarının eşleştirilmesi:

O anki faaliyet geliştikçe olan olayları ağaç dizileri ile birbirine bağlanır.eğer ağaç saldırının sonuna kadar artmakta ise bu sistemin kapanması ile sonuçlanır.

6) Sonuç

En iyi saldırı tespit programları, saldırılar karşısında karar verme mekanizmaları olarak paket seviyesi bilgisi veya kullanıcı seviyesi faaliyetleri kullanırlar.Bu makalede ağı devamlı olarak değişik katmanlarda (kullanıcı, işlem ve paket seviyesi) gözden geçiren ve hem amaç dışı kullanımı hem de dış saldırıları ayrıştırabilen bir saldırı tespit sisteminden bahsettik.

Bu sistemin, sistem güvenilirliğini arttıran, kendine özel algoritmaya sahip olma gibi kendine özel özellikleri bulunmakta idi.'b ' ve 'k' değerlerinin birbirine yakınlığı da ayrıca yanlış alarmları en aza indirmekte idi.

Bu tur bir saldırı tespit sistemi sizin de fark edebileceğiniz gibi geleceğin popüler ve güvenilir sistemi olmaya aday. Su anda hala özel testleri devam etmekte olan bu özel saldırı tespit sistemleri bakalım geleceğin internetini daha güvenli hala getirebilecekler mi?

7) Referanslar

- Anderson, J. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort

Washington, Pennsylvania, April 1980.

- Lunt, T.F.: Automated Audit Trail Analysis and Intrusion Detection: A Survey. 11th National Computer Security Conference, October, 1988 .
- Lunt, T.F.: Detecting Intruders in Computer Systems. 1993 Conference on Auditing and Computer Technology.
- Dasgupta, D., Gonzalez, F.A. : An Intelligent Decision Support System for Intrusion Detection and Response .
- Crosbie, M., Spafford, G. :Applying Genetic Programming to Intrusion Detection. COAST Laboratory, Purdue University, (1997) (also published in the proceeding of the Genetic Programming Conference).
- Anderson, D., Frivold, T., Valdes, A.: Next-generation Intrusion Detection Expert System (NIDES) :A Summary. Computer Science Laboratory SRI-CSL-95-07, May 1995.
- <http://www.cerias.purdue.edu/coast/intrusion-detection/welcome.html>
- Goldberg: Genetic Algorithms in Search, Optimization & Machine Learning.
- <http://www.stanford.edu/~milaps/projects/>
- <http://dares.enst-bretagne.fr/dares2004/Session3/paper10.pdf>
- http://www.isoc.org/isoc/conferences/inet/01/CD_proceedings/Foukia/inet.pdf
- Makale`nin tamamlanması sırasındaki yardım ve desteğinden dolayı Özkan Kırık`a teşekkürler.

Özgür Özdemircili

<http://www.enderunix.org>

<http://news.enderunix.org>

<http://haber.enderunix.org>

Sorularınız için : ozgur@enderunix.org