

**Bilgisayar-Bilgi Güvenliği ve Yönetimi/ BM-302**

**Prof.Dr. Abdulsamet HAŞILOĞLU**

**Hazırlayan**

**TUNA AYYILDIZOĞLU**

**130757023**

**Centralized Authentication Services**

**(RADIUS, TACACS, DIAMETER)**

**William Stackpole, CISSP**

**İçindekiler**

1. **AAA Hizmetinin Temel Özellikleri**
2. **RADIUS: Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti**
3. **TACACS: Terminal Erişim Kontrol Geçiş Kontrol Sistemi**
4. **ÇAP: İki kez RADIUS?**
5. **Erişim Kontrollerinin Uygulanması**
6. **AAA Hizmetinin Temel Özellikleri**

Merkezi bir AAA hizmetinin temel özellikleri (1) dağıtılmış (müşteri / sunucu) güvenlik modeli, (2) doğrulanmış işlemler, (3) esnek kimlik doğrulama mekanizmaları ve (4) genişletilebilir bir protokol içerir. Dağıtılmış güvenlik, kimlik doğrulama işlemini iletişim işleminden ayırır ve kullanıcı kimlik doğrulama bilgilerini tek bir merkezi veritabanında birleştirmeyi mümkün kılar. Ağ erişim cihazları (yani bir NAS) istemcilerdir. Kullanıcı bilgilerini bir AAA sunucusuna iletirler ve sunucunun döndürdüğü yanıtlara göre hareket ederler. Sunucular, kullanıcı bağlantı isteklerini alır, kullanıcıyı doğrular ve kullanıcıya hizmet vermek için gereken konfigürasyon bilgilerini NAS istemcisine geri gönderir. İade edilen bilgiler arasında taşıma ve protokol parametreleri, ek kimlik doğrulama gereklilikleri (yani geri arama, SecureID), yetkilendirme direktifleri (yani, izin verilen hizmetler, uygulama izinleri) ve muhasebe gereksinimleri yer alabilir.

İşlemlerin bütünlüğünü sağlamak için müşteri ile sunucu arasındaki aktarımlar doğrulanır. Hassas bilgiler (örneğin şifreler) gizliliği sağlamak ve şifreler ile diğer kimlik doğrulama bilgilerinin iletim sırasında izlenmesini veya yakalanmasını önlemek için paylaşılan bir gizli anahtar kullanılarak şifrelenir. Bu, veriler kamuya açık taşıyıcı (örn., WAN) bağlantıları arasında dolaşırken özellikle önemlidir.

AAA sunucuları çeşitli kimlik doğrulama mekanizmalarını destekleyebilir. Bu esneklik kilit bir AAA özelliğidir. Kullanıcı erişimi, PAP (Parola Doğrulama Protokolü), CHAP (Challenge El Sıkışma Kimlik Doğrulama Protokolü), standart UNIX oturum açma işlemi veya sunucu kullanılarak kimliği doğrulanabilir ve bir proxy görevi yapabilir ve kimlik doğrulamasını Microsoft etki alanı denetleyicisi, Novell gibi diğer mekanizmalara iletebilir NDS sunucusu veya bir SecureID ACE sunucusu. Bazı AAA sunucu uygulamaları, daha güvenli bağlantılar için arama numarası tanımlama (arayan kimliği) ve geri arama gibi ek mekanizmalar kullanır.

Teknoloji çok hızlı değiştiğinden, AAA sunucuları genişletilebilir protokollerle tasarlanmıştır. RADIUS, DIAMETER ve TACACS, protokolün mevcut uygulamalarını aksatmadan herhangi bir sayıda yeni parametreyi desteklemek için tasarlanmış değişken uzunluklu nitelik değerleri kullanır. DIAMETER’ın çerçeve yaklaşımı, herhangi bir sayıda özelleştirilmiş AAA modülünü destekleyebilecek bir taşıma mekanizmasını (çerçeve) standartlaştırarak ek genişletilebilirlik sağlar. Yönetim açısından bakıldığında, AAA sunucuları aşağıdakiler de dahil olmak üzere bazı önemli avantajlar sağlar:

• Kullanıcılar tek bir ana bilgisayarda tutulduğundan, daha az kullanıcı ayarı ve bakım süresi

• Daha az yapılandırma hatası çünkü formatlar birden fazla erişim cihazında benzerdir

• Öğrenilecek sadece bir sistem sözdizimi olduğundan daha az güvenlik yöneticisi eğitim gereksinimi talepler tek bir sistemden gelir

• Azaltılmış yardım masası çağrıları, çünkü kullanıcı arayüzü tüm erişim metotları arasında tutarlılık gösterir

• Erişim bilgilerinin daha hızlı çoğalması, çünkü bilginin yalnızca sınırlı sayıda AAA sunucusuna kopyalanması gerektiğinden kimlik doğrulama mekanizmaları (yani, SecureID)

• Genişletilebilir tasarım, mevcut kısıtlamaları bozmadan yeni cihazlar eklemeyi kolaylaştırır

1. **RADIUS: Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti**

RADIUS, günümüzde kullanılan en popüler AAA hizmetidir. Popülerliği, Livingston’un RADIUS kaynak kodunun dağıtımını açma kararına bağlanabilir. Kullanıcılar hizmeti birden fazla platformda hızlı bir şekilde sunmakta ve çoğu Livingston'un sonraki sürümlerde standart özellikler olarak dahil ettiği özelleştirilmiş özellikler eklemektedir. Bugün, RADIUS sunucusunun sürümleri, hem ücretsiz hem de ticari kaynaklardan gelen her büyük işletim sistemi için mevcuttur ve RADIUS istemcisi, her büyük satıcının NAS ürünlerinde standarttır.

Temel bir RADIUS sunucusu uygulaması iki konfigürasyon dosyasına referansta bulunur. Müşteri konfigürasyonu, müşterinin adresini ve işlemleri doğrulamak için kullanılan paylaşılan sırrı içerir. Kullanıcı, kullanıcı tanımlama ve doğrulama bilgilerini (örneğin, kullanıcı kimliği ve şifre) ile bağlantı ve yetkilendirme parametrelerini içerir. Parametreler, istemci ve sunucu arasında, tek bir UDP paketine yerleştirilmiş basit bir alan formatı kullanılarak iletilir. Biçimin kısaltması ve UDP protokolünün verimliliği (bağlantı yükü yok) sunucunun büyük miktarda istekleri verimli bir şekilde yerine getirmesine olanak tanır. Bununla birlikte, format ve protokol de bir dezavantaja sahiptir. Bugünün çeşitli erişim gereksinimlerinin (yani, ROAMOPS) bazılarına kendilerini iyi borç vermezler ve yeniden iletimler ağır yük veya başarısız düğüm senaryolarında bir sorundur.

**2.1. AA'yı RADIUS'a Koymak: Doğrulamalar ve Yetkiler**

RADIUS'ta sekiz standart işlem türü vardır: erişim isteği, erişim kabulü, erişim reddetme, muhasebe talebi, muhasebe yanıtı, erişim sorgusu, durum sunucusu ve durum istemcisi. Kimlik doğrulama, bir NAS erişim talebi paketinin şifresini çözmek, NAS kaynağını doğrulamak ve erişim talebi parametrelerini kullanıcıya göre doğrulamak suretiyle gerçekleştirilir. Sunucu daha sonra üç kimlik doğrulama yanıtından birini döndürür: erişim kabul, erişim reddet veya erişim mücadelesi. Sonuncusu, belirteci veya geri arama tanımlayıcısından bir defalık şifre gibi ek doğrulama bilgileri için bir istektir.

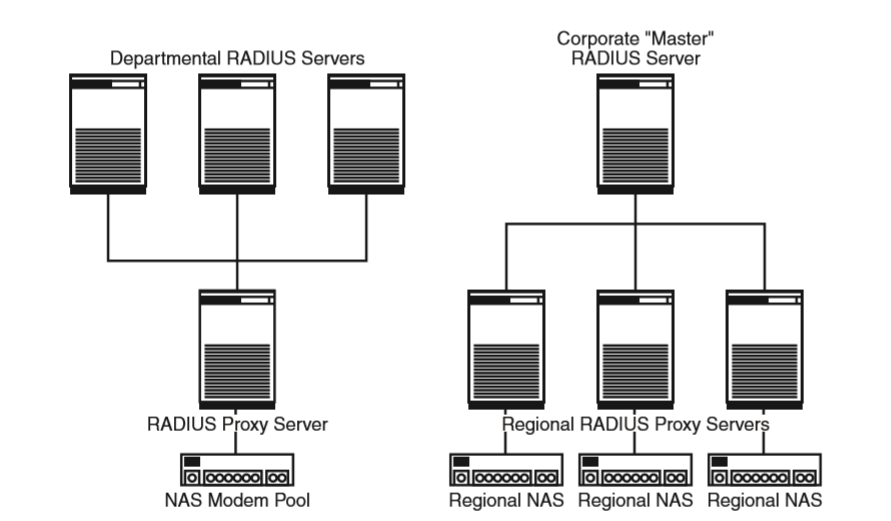
Yetkilendirme, RADIUS protokolünde ayrı bir fonksiyon değildir, sadece bir doğrulama cevabının bir parçasıdır. Bir RADIUS sunucusu bir erişim isteğini doğruladığında, kullanıcı istemcisinde belirtilen tüm bağlantı niteliklerini NAS istemcisine geri gönderir. Bunlar genellikle veri bağlantısı (yani, PPP, SLIP) ve ağ (yani, TCP / IP, IPX) özelliklerini içerir, ancak aynı zamanda satıcıya özel yetki parametreleri de içerebilir. Böyle bir mekanizma, belirtilen bir ana bilgisayara otomatik olarak bir Telnet veya rlogin oturumu başlatır. Diğer yöntemler arasında, bağlantı noktasını sınırlı bağlantıya sahip belirli bir IP adresine zorlamak veya erişim bağlantı noktasına bir yönlendirme filtresi uygulamak sayılabilir.

* 1. **Üçüncü A: Eh, Bazen Yine de!**

Muhasebe, RADIUS'ta ayrı bir işlevdir ve tüm istemciler bunu uygulamaz. NAS istemcisinin RADIUS muhasebe kullanması istenirse, kullanıcının kimliği doğrulandıktan sonra bir Hesap Başlatma paketi ve kullanıcı bağlantıyı kestiğinde bir Hesap Durdurma paketi oluşturur. Accounting-Start paketi, NAS'ın sunduğu hizmet türünü, kullanılan portu ve servis verilen kullanıcıyı açıklar. Accounting-Stop paketi, Başlangıç paketi bilgisini çoğaltır ve geçen süre, bayt girişleri ve çıkışları, bağlantı kesme nedeni vb. Gibi oturum bilgilerini ekler.

* 1. **İleri Düşünme ve Diğer Gee-Whiz Yetenekleri**

Bir RADIUS sunucusu, istemci istekleri için bir proxy görevi görebilir ve bunları diğer kimlik doğrulama alanlarındaki sunuculara iletir. Yönlendirme, adlandırılmış veya sayı alanı dahil olmak üzere bir dizi kritere dayalı olabilir. Bu özellikle departmanlar veya kuruluşlar arasında tek bir modem havuzu paylaşıldığında kullanışlıdır. Varlıkların kimlik doğrulama verilerini paylaşması gerekli değildir; her biri modem havuzundaki sunucudan kendi RADIUS sunucusunu ve hizmet proxy isteklerini koruyabilir. RADIUS, hem kimlik doğrulama hem de muhasebe isteklerini proxy yapabilir. Proxy'ler arasındaki ilişki dağıtılabilir (bire çok) veya hiyerarşik (çoktan bire) olabilir ve istekler birden çok kez iletilebilir. Örneğin, Ek 8.2'de, “ana” sunucunun kullanıcının işleme almak için bölgesel sunucusuna bir istek iletmesine mükemmel şekilde izin verilir. Çoğu RADIUS istemcisi, ikincil bir RADIUS sunucusunu artıklık amacıyla sorgulama yeteneğine sahiptir, ancak bu gerekli değildir. Birincil sunucu çevrimdışı olduğunda avantaj, erişimin devam etmesidir. Dezavantajı, sunucular arasında veri senkronize etmek için gereken yönetimdeki artıştır.



* 1. **Tökezleyen Bloklar, Karmaşıklıklar ve Diğer RADIUS Sınırlamaları**

RADIUS, uzaktan erişim kimlik doğrulaması için iyi çalışır ancak ana bilgisayar veya uygulama kimlik doğrulaması için uygun değildir. Web sunucuları ilk istisna olabilir. Bir RADIUS istemcisini bir Web sunucusuna eklemek, açık ağlardaki kullanıcıların kimliklerini doğrulamak için güvenli bir yöntem sağlar. RADIUS, yalnızca çivilenmiş devreleri veya sistem olaylarını izlemek için hiçbir imkan olmayan basit muhasebe olanakları sağlar. Cihaz tabanlı bağlantı parametreleri yerine kullanıcı bazlı RADIUS'un bir başka önemli kısıtlamasıdır. Tek bir RADIUS sunucusu birkaç farklı NAS cihazı türünü yönettiğinde, kullanıcı yönetimi oldukça karmaşıktır. Standart RADIUS kimlik doğrulaması, bir kullanıcının grup üyeliğini kontrol etmek, günün tarihine veya saatine göre erişimi kısıtlamak veya bir kullanıcının hesabını belirli bir tarihte sona erdirmek için kolaylıklar sağlamaz. Bu özellikleri sağlamak için, RADIUS sunucusunun ikincil bir kimlik doğrulama servisiyle ilişkilendirilmesi gerekir. Genel olarak, RADIUS, ek hesap kısıtlamalarının uygulanabileceği NDS veya NT gibi ikincil bir kimlik doğrulama hizmeti ile ilişkilendirildiğinde en iyi şekilde çalışan etkili, esnek ve iyi desteklenmiş bir AAA hizmetidir. RADIUS sürüm 2'nin bir IETF standardı olarak benimsenmesi, iyi bir genel amaçlı kimlik doğrulama, yetkilendirme ve muhasebe hizmeti olarak devam eden başarısını ve önemini kesinlikle sağlayacaktır.

1. **TACACS: Terminal Erişim Kontrol Geçiş Kontrol Sistemi**

Günümüzde TACACS olarak bilinenler aslında protokolün iki evrimini temsil eder. ARPANet günlerinin başlarında geliştirilen orijinal TACACS çok sınırlı bir işlevselliğe sahipti ve UDP taşımacılığını kullandı. 1990'ların başında, protokol ek işlevsellik içerecek şekilde genişletildi ve taşıma TCP'ye değiştirildi. Geriye dönük uyumluluk sağlamak için orijinal işlevler, genişletilmiş işlevlerin altkümeleri olarak dahil edildi. Yeni protokol XTACACS (Genişletilmiş TACACS) olarak adlandırıldı. Neredeyse tüm mevcut TACACS günlükleri RFC1492'de açıklandığı gibi genişletilmiş protokole dayanmaktadır. Cisco Systems, AAA mimarisi için TACACS'ı benimsedi ve kimlik doğrulama, yetkilendirme ve muhasebe işlevlerini ayırarak ve tüm NAS-sunucu iletimlerine şifreleme ekleyerek ürünü daha da geliştirdi. Cisco, kimlik doğrulama alışverişlerinde keyfi uzunluk ve içerik parametrelerine izin vererek TACACS'ın genişletilebilirliğini de geliştirdi. Cisco, TACACS + sürümünü seçti ancak gerçekte, TACACS + orijinal TACACS ile benzerlik göstermiyor ve paket formatları geriye dönük olarak uyumlu değil. Bazı sunucu uygulamaları uyumluluk amacıyla her iki formatı da destekler. Bu bölümün geri kalanı TACACS + 'ya dayanmaktadır, çünkü önerilen IETF standardıdır.

TACACS + sunucuları, sunucu seçeneklerini kontrol etmek, kullanıcıları ve nitelik / değer (AV) çiftlerini tanımlamak ve kimlik doğrulama ve yetkilendirme işlemlerini kontrol etmek için tek bir yapılandırma dosyası kullanır. Seçenekler bölümü, servisin çalışma parametrelerinin, paylaşılan gizli anahtarın ve muhasebe dosyasının adını belirtir. Dosyanın geri kalanı, kimlik doğrulama ve yetkilendirme işlemlerini kontrol etmek için kullanılan bir dizi kullanıcı ve grup tanımlamasıdır. Format, “user = username” veya “group = groupname”, ardından küme parantezleri içindeki bir veya daha fazla AV çiftidir.

**3.1. A 1: TACACS Kimlik Doğrulama**

TACACS kimlik doğrulamasının üç paket türü vardır: Başlat, Devam Et ve Yanıtla. İstemci, doğrulamaya, gerçekleştirilecek doğrulama tipini tanımlayan bir Başlangıç paketi ile başlar. PAP gibi basit kimlik doğrulama türleri için, paket aynı zamanda kullanıcı kimliğini ve şifreyi içerebilir. Sunucu bir Yanıtla ile yanıt verir. Gerekirse, ek bilgi istemciye Devam ve sunucu Yanıtla paketleriyle iletilir. İşlemler, oturum açma (ayrıcalık seviyesine göre) ve çeşitli kimlik doğrulama protokollerini (örneğin, CHAP, PAP, PPP, vb.) Kullanarak parola değişikliğini içerir. RADIUS gibi başarılı bir TACACS kimlik doğrulaması da bağlantı yapılandırması için özellik değeri (AV) çiftleri döndürür. Bunlar yetkilendirme parametrelerini içerebilir veya ayrı olarak alınabilir.

* 1. **A 2: TACACS Yetkilendirmesi**

TACACS'deki yetkilendirme işlevleri, aşağıdakiler için kullanılan İstek ve Yanıt AV çiftlerinden oluşur: • Belirli komutlara, adreslere, hizmetlere veya protokollere izin verme veya reddetme • Kullanıcı ayrıcalık düzeyini ayarlama • Giriş ve çıkış paketini filtrelemeyi • lterler • Erişim kontrol listelerini ayarla ( ACL'ler) • Geri arama eylemlerini çağırma • Belirli bir ağ adresi atama İşlevler, bir kimlik doğrulama işleminin veya yetkilendirme özel isteğinin bir parçası olarak döndürülebilir.

* 1. **A 3: TACACS Muhasebe**

Muhasebe işlevleri, yetkilendirme işlevlerine benzer bir format kullanır. Muhasebe işlevleri Başlat, Durdur, Diğer ve Bekçi köpeğidir. Watchdog işlevi, veriler uzun süre boyunca gönderilmediğinde, TCP oturumlarını doğrulamak için kullanılır. RADIUS tarafından desteklenen standart muhasebe verilerine ek olarak, TACACS, erişim haklarında veya ayrıcalıkta sistem düzeyinde değişiklikleri kaydedebilen bir olay günlüğü özelliğine sahiptir. Olayın nedeni ve bununla ilişkili trafik toplamları da kaydedilebilir.

* 1. **Proksilite, Sorunlar ve Tuzaklar**:

TACACS Sınırlamaları TACACS + 'ın prensip sınırlaması kullanım eksikliği olabilir. TACACS + çok yönlü ve sağlam bir protokol olmasına rağmen, daha az sunucu uygulaması ve daha az NAS uygulaması var. Cisco dışında, bu yazar protokolde herhangi bir özel uzantı veya satıcıya özgü AV çiftleri bulamadı. Ek olarak, TACACS’ın ölçeklenebilirliği ve performansı bir sorundur. RADIUS’un tek paket UDP tasarımından farklı olarak, TACACS, bağlantılar kurmak için TCP üzerinden birden çok sorgu kullanır, böylece performansı ciddi şekilde etkileyebilecek ek yükler ortaya çıkar. TACACS + sunucularının proxy istekleri yoktur, bu nedenle birden fazla etki alanında kimlik doğrulamayı desteklemek için bir hiyerarşide yapılandırılamazlar. CiscoSecure ölçeklenebilirliği, birden çok alanda ölçeklendirmek için bölgesel sunuculara ve veritabanı çoğaltmasına dayanır. Uygulanabilir olmakla birlikte, yaklaşım her zaman böyle olmayabilen tek bir yönetim alanı varsaymaktadır. Genel olarak, TACACS +, Cisco’nun NAS tabanlı VPN’lerin uygulanmasına yönelik mevcut desteği olan güvenilir ve oldukça genişletilebilir bir protokoldür. “Outcalls” özelliği, AAA işlevlerini kişiselleştirmek ve üçüncü taraf ürünlere destek eklemek için oldukça basit bir yol sağlar. TACACS +, RADIUS'tan daha fazla kimlik doğrulama parametresini desteklese de, NDS veya bir NT alanı gibi ikincil bir kimlik doğrulama servisiyle ilişkilendirildiğinde en iyi şekilde çalışır. TACACS + 'ın bir IETF standardı olarak benimsenmesi ve kolay genişletilebilirliği, diğer NAS üreticileri tarafından benimsenmesini iyileştirmelidir. O zamana kadar, TACACS + Cisco merkezli ortamlar için sağlam bir AAA çözümü olmaya devam ediyor.

1. **ÇAP: İki kez RADIUS?**

DIAMETER, herhangi bir sayıda kimlik doğrulama, yetkilendirme veya muhasebe planı ve bağlantı türünü destekleyebilen oldukça genişletilebilir bir AAA çerçevesidir. Protokol iki ayrı bölüme ayrılmıştır: Temel Protokol ve Eklentiler. DIAMETER Baz Protokolü, tüm DIAMETER uzantıları tarafından kullanılan mesaj formatını, aktarımı, hata raporlamasını ve güvenlik servislerini tanımlar. DIAMETER Eklentileri, belirli tip kimlik doğrulama, yetkilendirme veya muhasebe işlemlerini (yani NAS, Mobile-IP, ROAMOPS ve EAP) yapmak için tasarlanmış modüllerdir. Mevcut IETF taslağı, NAS talepleri, Mobil IP, güvenli proxy, güçlü güvenlik ve muhasebe için açıklamalar içerir, ancak herhangi bir sayıda başka uzantı mümkündür. DIAMETER, RADIUS protokolü üzerine kuruludur, fakat doğal RADIUS sınırlamalarını aşması için artırıldı. İki protokol ortak bir veri birimini (PDU) paylaşmasa da, RADIUS'tan DIAMETER'e geçişi kolaylaştırmak için uygun benzerlikler vardır. DIAMETER, RADIUS gibi bir UDP aktarımı kullanır, ancak istemci / sunucu yapılandırmasından ziyade eşler arası. Bu, sunucuların istekleri başlatmasına ve iletim hatalarını yerel olarak işlemesine izin verir. DIAMETER, yeniden iletimi azaltmak, başarısız düğüm tespitini iyileştirmek ve düğüm tıkanıklığını azaltmak için güvenilir taşıma uzantıları kullanır. Bu geliştirmeler gecikmeyi azaltır ve yüksek yoğunluklu NAS ve hiyerarşik proxy yapılandırmalarında sunucu performansını önemli ölçüde artırır. Ek iyileştirmeler şunları içerir:

• Dolaşım için tam destek • Alan etki alanı, broker temelli kimlik doğrulama

• Genişletilebilir Kimlik Doğrulama Protokolü (EAP) için tam destek • Satıcı tarafından belirlenen nitelik-değer çiftleri (AVP'ler) ve komutlar

• Tekrarlanan saldırı korumaları ve gizliliği ile geliştirilmiş güvenlik işlevselliği bireysel AVP'ler için

**4.1. İki Brute: ÇAPETİ Yetkilendirme işlemleri**

Kimlik doğrulama talepleriyle birleştirilebilir veya ayrıca gerçekleştirilebilir. İşlemin özellikleri kullanılan Uzantı tarafından yönetilir ancak aynı modeli izler ve aynı komutları kimlik doğrulama olarak kullanır. Yetkilendirme talepleri mevcut bir oturumda gerçekleştirilmelidir; oturum başlatmak için kullanılamazlar, ancak bir DIAMETER proxy'si kullanılarak iletilebilirler.

* 1. **Her Şey için Muhasebe**

DIAMETER, olay izleme, periyodik raporlama, gerçek zamanlı kayıt transferi ve ROAMOPS Muhasebe Veri Değişim Biçimi (ADIF) desteği ekleyerek, RADIUS ve TACACS + 'nın muhasebe yeteneklerini önemli ölçüde geliştirir. ÇAPI muhasebe, yetkilendirme-sunucuya yöneliktir. Müşterinin muhasebe kayıtlarını nasıl üreteceğine ilişkin talimatlar, yetkilendirme sürecinin bir parçası olarak müşteriye iletilir. Ek olarak, DIAMETER muhasebe sunucuları bir müşteriyi mevcut muhasebe verilerini göndermeye zorlayabilir. Bu özellikle bağlantı sorunlarını gidermek veya bir muhasebe sunucusu bir çökme ile karşılaştığında muhasebe verilerini yakalamak için kullanışlıdır. İstemci yazarları ve sunucu anketleri her iki DIAMETER proxy modelinde tam olarak desteklenir. Verimlilik için, kayıtlar normalde parti aktarılır, ancak kredi limiti kontrolleri veya sahtekarlık tespitinin gerekli olduğu ROAMOPS gibi uygulamalar için, kayıtlar gerçek zamanlı olarak oluşturulabilir. DIAMETER, çivilenmiş devrelerde kullanımın izlenmesi için özellikle yararlı olan periyodik raporlama özelliğine sahip standart bağlantı ve bağlantı kesme hesaplarını geliştirir. DIAMETER ayrıca, başarısız düğümler ve sunucu yeniden başlatmaları gibi servisle ilgili olayları kaydetmek için yararlı olan TACACS + gibi bir olay muhasebesi özelliğine de sahiptir.

* 1. **Güvenlik, Standartlar ve Diğer Öğeler Güçlü Güvenlik Desteği**

DIAMETER Baz Protokolünün standart bir parçasıdır. ROAMOPS ve Mobile-IP gibi birçok uygulama, birden çok alanda aktarılması için hassas bağlantı bilgileri gerektirir. Atlamalı atlama güvenliği bu uygulamalar için yetersizdir, çünkü veriler her ara atlamada maruz kalmaya maruz kalmaktadır. DIAMETER’ın Güçlü Proxy Uzantısı, S / MIME nesnelerindeki hassas verileri şifreleyerek ve bunları standart AVP’lerde bulundurarak sorunun üstesinden gelir. Telekomünikasyon, mobil işgücü, VPN, çoklu platform, içeri arama kullanıcı kimlik doğrulama blues'ları var mı? Birinin buna ihtiyacı yok! RADIUS, TACACS ve DIAMETER gibi AAA sunucu çözümleri bu blues'ları kovalayabilir. Biraz dikkatli bir planlama ve birkaç saatlik bir yapılandırma ile, güvenliği artırmak, yönetim zamanını azaltmak ve birinin uzaktan erişim mekanlarını tek, merkezi, esnek ve ölçeklenebilir bir çözümde birleştirmek mümkün olabilir. Bu birinin yüzüne bir gülücük vermeli.

**5.Erişim Kontrollerinin Uygulanması**

**Stanley Kurzban**

Hangi erişim kontrollerinin uygulanacağı kararı organizasyon politikasına ve genel olarak kabul görmüş iki uygulama standardına dayanmaktadır: görevlerin ayrılması ve en az ayrıcalık. Kontrollerin kabul edilmesi ve

Bu nedenle, etkili bir şekilde kullanıldığında, normal iş akışını daha fazla bozmamalı

gereğinden fazla veya yöneticilere, denetçilere çok fazla yük getirmesi,

veya yetkili kullanıcılar.

Erişim denetimlerinin kuruluşun tüm kaynaklarını yeterli şekilde koruduğundan emin olmak için, önce kaynakları sınıflandırmak gerekebilir. Bu

Bölüm bu süreci ve çeşitli erişim kontrol modellerini ele almaktadır.

Katılımsız oturumlar üzerinde kontrol sağlama yöntemleri de tartışılmış ve erişim kontrollerinin yönetimi ve uygulanması

incelemiştir.

* 1. **KATEGORİ KAYNAKLARI**

Politikalar, veriler ve diğer kaynaklar için hassasiyet seviyeleri (örneğin, çok gizli, gizli, gizli ve sınıflandırılmamış) belirler. Bu seviyeler olmalı

Verilerin işlenmesi için uygun prosedürler konusunda rehberlik etmek için kullanılır - örneğin, kopyalanmaması için talimatlar. Erişim kontrolü kararları için de temel olarak kullanılabilirler. Bu durumda, bireylere yalnızca erişim yetkisi verilir

bu kaynaklar belirli bir hassasiyet seviyesinde veya altındadır. Etiketler kullanılıyor

Elektronik olarak depolanan belgelerin hassasiyet seviyesini göstermek için.

Ek olarak, erişim kontrol politikası kaynakların bölümlere ayrılmasına dayalı olabilir. Örneğin, erişim kontrollerinin tümü belirli bir projeyle veya belirli bir çaba alanıyla (örneğin, teknik Ar-Ge veya

askeri istihbarat). Erişim kontrollerinin uygulanması şunları içerebilir:

tek bölmeler veya bunların kombinasyonları. Bu birimleri

“bölme” terimi ve buna rağmen kategoriler denir.

“Kategori” genellikle birbirinin yerine kullanılır. Her iki terim de veri işleme kısıtlamaları için geçerli değildir. Bireyler, bir kaynağa erişim hakkına sahip olmak için bir kaynakla ilişkili tüm kategoriler için yetkilendirmeye ihtiyaç duyabilir (bu durumda olduğu gibi).

© 2004, CRC Press LLC tarafından

ABD hükümetinin sınıflandırma şeması) veya kategorilerin herhangi birine (diğer kuruluşların çalışma şeklini daha fazla temsil ettiği gibi).

* 1. **Nesne Oluşturma**

Yeni bir nesne oluşturulduğunda, ona ne tür erişime izin verildiğine şüphe olmamalıdır. Oluşturma işi veya oturumu belirtebilir

açıkça bilgi; ancak, birileri adına hareket ettiğinden

Yönetici olmayabilir, zorunlu olanlara aykırı olmamalıdır

politikaları. Bu nedenle, yeni oluşturulan nesne hassasiyeti üstlenmelidir

İçerdiği verilerin Veriler kaynaklardan toplanmışsa

farklı özellikler, zorunlu politikanın dışlayıcı niteliği

Yeni nesnenin, verilerinin elde ettiği en hassas nesnenin özelliklerini üstlenmesini gerektirir.

* 1. **Veri Sınıflandırmalarını Düşürme**

Veri sınıflandırmalarının düşürülmesi bir yönetici tarafından gerçekleştirilmelidir. Bir iş veya oturum, yönetici olmayan biri adına hareket edebileceği için, veri sınıflandırmalarını düşürmemelidir. sağlanması

yeni nesnelerin en hassas nesnenin özelliklerini aldığını

verilerinin türetildiği bu amaca hizmet eden bir güvencektir.

Diğer bir koruma, bir işin veya oturumun çıktısı ile ilgilidir - çıktı

asla en hassas seviyenin altındaki bir nesneye yazılmamalıdır

kullanılan iş veya oturum. Bu, ilgili veriler olabilir.

işin veya oturumun hassasiyet seviyesinin çok altında bir duyarlılığa sahip olmak,

Çünkü bireysel verileri izlemek her zaman mümkün değildir. Bu gibi görünebilir

pratik olmayan sert bir önlem; ancak en iyi niyetli olanlar bile

kullanıcılar yetkileri ile hareket eden bir Truva atı tarafından kandırılabilirler.

Savunma Bakanlığı’nın (DoD’lar) alanı dışında,

okunan verilere, bu verileri daha düşük hassasiyette bir dosyada saklayarak sınıflandırmalarını düşürme ayrıcalığı verilir. Bu mümkün

büyük ölçüde, çünkü verilerin toplanması, aralarındaki verilerin ayrı maddelerine göre daha hassas olabilir. Medeni hukukun geçerli olduğu durumlarda, özellikle DoD düzenlemeleri tarafından onaylanan fiili yükseltme,

Ciddi düşünce. Örneğin, mahkemeler sır hırsızlığını tedavi edebilir

tuvalet onarımı bildirimleri gizli olarak etiketlenirse verileri hafifçe. Bununla birlikte,

hiç kimse, fiili olarak yükselmeye karşı güvence altına almadı.

* 1. **Etiketleme**

Bir işten veya oturumdan çıktı, manyetikten ziyade fiziksel olduğunda veya

Elektronik, hassasiyeti açıklayan bir etiket taşımalıdır ki insanlar

uygulanabilir politikalara uygun olarak kullanabilir. Etiketler olabilir rağmen

hacimli olmak ve bu nedenle fiziksel anlamda sinir bozucu olmak

etiket yanlış yerleştirilmişse ciddi sorunlar yaratabilir.

Örneğin, etiketlere bakılmaksızın yazılmış bir program veri yerleştirebilir

çıktı ortamındaki herhangi bir noktada - örneğin basılı bir sayfa. Bir etiket

isteğe bağlı olarak o sayfaya sabit bir konuma yerleştirildiğinde değerli bir yer paylaşımı olabilir

etiketten daha fazla zarara neden olan verilerin önlenmesi beklenebilir. Etiketi, bir tane bile olsa boş boyutta boş bir yere yerleştirmek,

Amaca hizmet et çünkü kimse onu nerede arayacağını bilemeyebilir.

yanlış etiket sayfanın başka bir yerinde görünebilir.

Çünkü her bir çıktı sayfasını etiketlemek bu kadar zor problemler doğurur,

tüm yazdırma dosyalarının etiketlenmesi özellikle önemlidir. Kolay olmasına rağmen

Bir dosyayı bir sayfa ile açıklayan ve izleyen bir sayfa, böylesi bir sayfanın sahteciliğine karşı korunma daha kapsamlı önlemler gerektirir. Örneğin, bir kişi bir sayfanın ortasında bir sayfa oluşturabilir.

Bu dosyayı sonlandırmak için görünen çıktı dosyasını. Bu kişi daha sonra mümkün olabilir

tamamen ayrı, yanıltıcı etiketli bir dosyanın görünümünü simüle etmek

sahte sayfanın ardından. Başlık ve fragman sayfalarında öngörülemeyen ve işler için kullanılamayan bir rastgele sayı varsa, bu tür

sahtecilik mümkün değildir.

Etiketlerin tartışmaları genellikle duyarlılığı yansıtan etiketlere odaklanır

yetkisiz kişilerce gözlem, ancak etiketler hassasiyeti yansıtabilir

fiziksel kayıplara da. Örneğin, belirli bir dosya veya belgenin her zaman erişilebilir olmasını sağlamak, en azından sağlamak kadar önemli olabilir.

yalnızca yetkili kullanıcılar bu dosyaya veya belgeye erişebilir. Bu bölümde gizlilik bağlamında tartışılan tüm hususlar;

kullanılabilirliği iyi.

1. **ERİŞİM KONTROL MODELLERİ**

Erişim kontrol politikalarının sıkı bir şekilde incelenmesine izin vermek, çeşitli modeller politikalar geliştirilmiştir. Erken dönem çalışmaları, ABD hükümetinde yürürlükte olan politikaların ayrıntılı tanımlarına dayanıyordu; ticari kaygıları ele aldı. Aşağıdaki bölümler birkaç modelin genel görünümünü içermektedir.

* 1. **Kafes Modelleri**

Kafes modelinde, her kaynak ve bir kaynağın her kullanıcısı, sıralanan bir sınıf kümesinden biriyle ilişkilendirilir. Kaynaklanan sınıflar askeri isimler gizli, gizli, gizli ve sınıflandırılmamış. Belirli bir sınıfla ilişkili kaynaklar belki sadece ilişkili sınıfı, sınıfınınkinden daha yüksek veya daha yüksek olanlar kaynaklar. Bu planın resmi olarak sınıflandırılmış veriye uygulanabilirliği açıktır; bununla birlikte ticari ortamlarda uygulanması da uygun olur.

* 1. **Bell-LaPadula Modeli**

Kafes modeli, ortaya çıkacak tehdidi dikkate almamıştır. Belirli bir sınıfla ilişkili kişilerin kendileri için bilinmeyen bilgileri bir kaynağa kopyalayan bir programda gizlenen bir Truva atı daha düşük bir erişim seviyesi ile. Hükümet açısından, Truva atı Sınıflandırmanın fiili olarak düşürülmesinin etkili olduğu söylenebilir. Gerçeğe rağmen hiç kimsenin, şu ana kadar önemli bir kayıp yaşadığına dair hiçbir kanıt olmadığını böyle bir saldırının sonucu, böyle bir saldırı çok çekici olurdu ve Alandaki birkaç kişi bu konuda haklı endişeli. Bell ve LaPadula böyle bir saldırıyı dikkate alan bir model geliştirdi. Bell-LaPadula modeli, kullanıcıların ve işlemlerin okumasını önler kafes modelinde olduğu gibi güvenlik seviyelerinin üzerinde (yani, belirli bir sınıflandırmaya sahip işlemlerin daha yüksek bir değerle ilişkili verileri okuyamayacağını belirtir sınıflama). Buna ek olarak, ancak, herhangi bir verilen süreçleri önler. Daha düşük bir sınıflandırma ile ilişkili verileri yazmadan sınıflandırma. Bazıları, işlemin sınıflandırmasını aşağıda yazabilme yeteneğinin gerekli bir fonksiyon olduğunu düşünse de, hassas olmayan veriler yerleştirerek, Hassas bir belgede olsa da, daha az hassas bir dosyada Görmesi gereken insanlar için mevcut olabilir - DoD uzmanları bunu verdi fiili indirgeme tehdidine fazla ağırlık, model hissettiğini engellemek zorunda kaldım. Ulusal Bilgisayar Güvenliği tarafından desteklenen tüm çalışmalar Merkez (NCSC) bu modeli kullandı. “Yüksek” terimi, bu bağlamda, daha yüksek bir ifadeden daha fazlasını ifade eder. sınıflandırma - aynı zamanda tüm kaynak kategorilerinin bir üst grubunu da ifade eder. İçinde Bell-LaPadula modelinin ticari veri işlemeye uygulanabilirliğini öne süren Lipner, kategorilerin bir üst kümesi için olan gereksinimin hükümet çevreleri dışında uygun olamayacağından bahseder. Bell-LaPadula modeli bağlamında dikkate değer bir isimlendirme ortaya çıkmıştır. Okuma kısıtlamasına basit güvenlik özelliği denir. Yazma kısıtlaması, yıldız özelliği olarak adlandırılır, çünkü Mülkiyet daha resmi bir şekilde verilene kadar bir yer tutucu olarak kullanılan yıldız isim asla değiştirilmedi.

* 1. **Biba Modeli**

Bell-LaPadula modelinin iki özelliğini inceleyen Biba, yetkisiz değişikliklerin önlenmesi olarak tanımladığı makul bir bütünlük kavramı keşfetti. Elde edilen Biba bütünlük modeli bütünlüğün korunması, verilerin bir hazneden akmamasını gerektirir daha yüksek bütünlükteki bir hazneye bütünlük verildi. Örneğin, eğer bir işlem Güvenlik seviyesinin üzerine yazabilir, güvenilir veriler kirlenebilir daha az güvenilir veri ekleyerek.

* 1. **Take-Grant Modeli**

Denetçiler, kimin yapmaya yetkili olduğu ile ilgilenmeli Hangi verilere ne tür bir erişim sağlanabileceği, ayrıca hangi verilere izinsiz erişim sağlanamayabilir idari müdahale. Bu olmayan bazı insanlar olduğunu varsayar Yöneticiler, diğerlerine de yetki vermeye yetkilidir. isteğe bağlı erişim kontrolleri olduğunda durum. Alınan hibe modeli iptal etme sonuçlarını incelemek için matematiksel bir çerçeve sağlar ve yetkilendirme. Bu nedenle, denetçiler için kullanışlı bir analitik araçtır.

**6.5. Clark-Wilson Modeli**

Wilson ve Clark 1987’de bunu gözlemleyenlerin arasındaydı. erişim kontrolü modelleriyle ilgili akademik çalışma, verilerin bütünlüğünden ziyade gizliliğini vurguladı (yani, yetkisiz modifikasyona göre yetkisiz gözlem). Buna göre, ticari bir görüşe göre belirgin bir şekilde farklı olan askeri bir görüş olarak gördüklerini telafi etmeye çalıştılar. Aslında, ne onlar askeri görüşün askeriyede yaygın olmadığı düşünülmektedir. Clark-Wilson modeli konu / program / nesne üçlülerinden oluşur ve veri, uygulama programları ve üçlülerle ilgili kurallar. Aşağıdaki bölümler Üçlü ve kuralları daha ayrıntılı olarak tartışınız. Üç katına. Clark-Wilson'dan önceki tüm resmi erişim kontrol modelleri model sipariş edilen bir konu / nesne çiftini ele alır - yani bir kullanıcı ve bir öğe veya Sabit bir ilişkiye göre veri toplama (örneğin, okuma veya yazma) ikisinin arasında. Clark ve Wilson ilişkinin olabileceğini kabul ettiler keyfi bir program tarafından uygulanır. Buna göre, sipariş verilenleri konu / program / nesne üçlü. Programın bütünlüğünün uygunluğa sahip olduğunu açıkça ortaya koymak için program için “dönüşüm prosedürü” terimini kullanırlar. çünkü verileri bir kurala veya prosedüre göre değiştirir veya dönüştürür. Dönüşüm prosedürlerinin değiştirdiği verilere kısıtlanmış veriler denir. öğeler sadece dönüşümsel anlamda kısıtlı oldukları için prosedürler onları ve bu bütünlük doğrulama prosedürlerini değiştirebilir belirli özelliklere sahip olmalarını sağlamak için üzerlerinde kısıtlamalar kullanmak, gerçek dünyaya tutarlılık ve uygunluk en önemli. Sınırlandırılmamış veri öğeleri, tüm diğer verilerdir, özellikle dönüşümsel prosedürlere girdi girdi. Özneler bir kez kısıtlandıktan sonra, bunlara erişebilmeleri için Nesneleri yalnızca belirtilen dönüşüm prosedürleriyle, dönüşüm prosedürleri neye ihtiyaç duyulursa mantığa gömülebilir. ayrıcalık sınırlaması ve görevlerin ayrılması. Dönüşümsel prosedürler, öznelerin nesnelere düzeydeki nesnelere erişimini kontrol edebilir sisteme uygun olandan daha ince tanecikli Dahası, onlar daha hassas kontroller yapabilir (örneğin, makul olma ve tutarlılık kontrolleri) kısıtlanmamış veri öğeleri üzerinde) çift girişli defter tutma gibi amaçlar için, böylece bir hesaptan çıkarılmış olanın bir başkasına eklenir, böylece varlık işlemlerde korunur. Kurallar. Bütünlüğün elde edilmesini ve korunmasını sağlamak için Clark ve Wilson, bazı bütünlük izleme ve bütünlük koruma kurallarının gerekli. Bütünlük izleme kuralları sertifika kuralları ve bütünlük koruma kuralları uygulama kuralları olarak adlandırılır. Bu sertifikalandırma kuralları aşağıdaki kavramları ele almaktadır:

• Sınırlandırılmış veri öğeleri tutarlıdır.

• Dönüşüm prosedürleri geçerli şekilde hareket eder.

• Görevler ayrılmıştır.

• Girişler günlüğe kaydedilir.

• Sınırlandırılmamış veri öğeleri doğrulanır.

* 1. **Katılmamış Oturumlar**

Başka bir tür erişim kontrolü, katılımsız oturumlarla ilgilidir. Kullanıcılar

bilgisayarlarla sürekli etkileşime girerek saatlerce zaman geçiremiyorum

aynı liman; herkes sık sık ara vermeye ihtiyaç duyar. Kaynak odaklı ise

şifreler kullanılmaz, sistemler bir oturumun tüm işlemlerini ilişkilendirmelidir

başlatan kişiyle. Seans inhibitörü iken devam ederse

ara verir, başka biri gelip bunun içinde bir şeyler yapabilir

başlatıcının yetkisi ile oturum. Bu bir ihlal teşkil eder

güvenlik. Bu nedenle, kullanıcıların bilgisayarlarını iş istasyonlarından uzakta olduklarında oturum açmaları konusunda cesaretlendirilmeleri gerekir.

Yöneticiler kullanıcıların oturumlarına katılmasını istiyorsa, aşağıdakiler gereklidir:

• İnsanların işlerine ara vermelerini ve devam etmelerini kolaylaştırın.

• Sistemdeki devamsızlıkları tespit etmeye ve oturumu korumaya çalışın.

• Katılımsız iken ortamın fiziksel korunmasını kolaylaştırın.

• Kesinlikle insan kontrolleri uygulamak (örneğin;

suçluları tespit etmek için personel).

Kullanıcılar her zaman oturumu kapatsa, katılımsız oturum olmazdı

limanlarını terk ettiler. Çoğu kullanıcı bunu yapmaz çünkü giriş yapmaları gerekir

geri döndüğünüzde, tipik bir sistemin oturum açma işlemi ne basit ne de

hızlı. Bu eksikliği telafi etmek için bazı kuruluşlar hızlandırılmış

oturum açma / kapatma programları, ayrıca askıya alma programları da denir. Askıya alma programları

port arasındaki fiziksel veya mantıksal bağlantının hiçbir bölümünü kesmeyin

ve bir konukçu; aksine, bağlantıyı sürdüren kaynakları keserler.

Ana bilgisayarın bağlantı noktası askıya alınmış bir duruma getirilmesini sağlar. Liman serbest bırakılabilir

askıya alınmış durumdan yalnızca bir parola veya başka bir kimlik doğrulama mekanizması sağlayarak. Bu kullanıcılar için daha elverişli olduğundan, kuruluşlar çalışanları izinli kullanmak yerine kullanmaya teşvik edeceğini umuyor

oturumları katılımsız.

UNIX'in kilit işlevi bir askıya alma programına bir örnektir. Kullanıcılar yapabilir

oturumu askıya alırken bir şifre girin ve aynı şifreyi tekrar girerek tekrar başlatın. Şifre, kullanıcının oturum açması olmamalıdır

Şifre, bir davetsiz misafir, kullanıcının oturumu sırasında yeni bir oturum başlatabildiğinden

kilit fonksiyonunu taklit edecek bir programın bulunmaması ve çalıştırılması, ardından

Kullanıcının özgeçmiş şifresini oku ve davetsiz misafirlerin kendi şifrelerinde sakla

oturum sonlandırma arızasını simüle etmeden önce dosyalar.

Katılımsız oturumları önlemenin başka bir yolu da kullanıcıları kendi zincirleriyle zincirlemektir.

oturumları. Örneğin, eğer bir liman kilitli bir kapısı olan bir ofiste ise

Ne zaman serbest bırakılırsa ve sadece bir kişi her kapının anahtarı varsa,

bir sistem mekanizmasına sahip olmak gerekli değildir. Kimliklerin tespiti için eserler kullanılıyorsa ve eserler sahiplerine aittir (örneğin hassas devlet binalarındaki kimlik kartlarına benzer şekilde),

Yapının çıkarılması, bir oturumun otomatik olarak sonlandırılmasını tetikleyebilir. İçinde

daha yaygın ortamlarda, en iyi çözüm, bazı farklılıklar olabilir.

devamındaki:

• Bağlantı noktasından, zil veya başka bir sinyal olmadan beş dakika geçerse

cihaz sesleri

• Sinyal olmadan başka bir yarım dakika geçerse,

zaman aşımı adı verilen oturum gerçekleşir.

Bir kullanıcı işlem yapmazsa sistem otomatik olarak oturumu sonlandırabilir

Yönetici tarafından belirtilen bir süre boyunca (örneğin, beş dakika). böyle

Bununla birlikte, bir tehlike tehlikesi vardır. Örneğin, kullanıcılar kilitlendi

(yani, sistemin hissedebileceği herhangi bir şekilde davranması engellenmiştir) uzun süren işlemlerle oturumlarını gereksiz yere sonlandırırlar. Ek olarak,

kullanıcılar programın altındaki bir işlemi simüle ederek kontrolü atlayabilir

kontrol, oturum sonlandırılmasını önlemek için yeterince sık.

**6.7. KONTROL YÖNETİMİ**

Erişim kontrollerinin yönetimi, erişim kontrol kurallarının oluşturulmasını ve sürdürülmesini içerir. Bu hayati bir endişe çünkü eğer bu tür

yönetim zordur, kötü yapılması kesindir. Etkili yönetimin anahtarı:

• Kuralları mümkün olduğunca ekonomik ve doğal olarak ifade etmek.

• Mümkün olduğunca çok alakasız ayrımdan habersiz kalmak.

• İdari kapsamın yönetilebilir yargı alanlarına indirgenmesi (yani,

yerinden).

Kurallar, gruplama mekanizmaları kullanılarak ekonomik olarak ifade edilebilir. Yönetici arayüzleri, yöneticilerin mecburi olmadıklarını temin eder

alakasız ayrımlarla uğraşın ve idari kapsamın azaltılmasına yardımcı olun.

Aşağıdaki bölümlerde gruplama ve yönetici arayüzleri tartışılmaktadır.

**6.8. Gruplandırma Konuları ve Nesneleri**

Söylenmesi gereken şeyin azaltılması iki yönü içerir: nesnelerin gruplandırılması ve

gruplama konuları. Kaynak kategorileri gruplandırmanın bir yolunu gösterir

nesneler. Başka bir mekanizma adlandırmadır. Örneğin, bir kullanıcının tüm özel

nesneler, kullanıcının tanımlayıcıları içinde kendi adını taşıyabilir. Bu durumda,

Bir kullanıcının tüm bunlara her türlü erişime sahip olabileceğini belirten tek bir kural

kullanıcının kendi özel nesneleri, binlerce veya hatta milyonlarca ayrı erişim izni ifadesinin yerini alabilir. Yine başka bir yol

nesneler gruplarına göre gruplandırılmıştır; Bu durumda, yöneticiler tüm manyetik bant hacimlerini veya tüm CICS işlemlerini sınıflandırabilir. Hala diğer

Nesneleri gruplandırma yöntemleri cihaz, dizin ve kütüphanedir.

Konu grupları kategorilerle eşleştiğinde, birçok izin

Tüm gruplara veya seçilen erişim türlerine grup veren tek bir kuralda belirtilmiştir.

belirli kategorilerin kaynaklarına. Çeşitli idari amaçlar için,

ancak, gruplar kategorileri temsil etmeyebilir; aksine, temsil etmeleri gerekir

organizasyon departmanları veya olmayan diğer gruplar (örneğin, projeler)

kategoriler. Her ne kadar konu gruplama ayrıcalık standardına göre çalışsa da, kimlik tabanlı erişim kontrolü dengeyi yeniden düzenler.

**6.9. Yönetici Arabirimleri**

Alakasız ayrımlardan habersiz kalmak için, yöneticilerin

tutarlı ve tutarlı bir arayüz. Arayüzün ne ile tutarlı olduğu

idari içeriğe bağlıdır. Yöneticiler birden fazla işlem yaparsa

alt sistemlerde, tek bir ürün yöneticilere tek bir ürün sağlayabilir

Temin ettikleri alt sistemlerin çeşitliliğini gizleyen arayüz

idari veri. Öte yandan, yöneticiler bekarlarla ilgilenirse

alt sistemler, alt sistemin kendisi veya alt sisteme özgü bir ürün, yöneticilere idari ve diğer işlemleri yapan bir arayüz sağlayabilir

onlara sunulan fonksiyonlar.

İdari yük, eğer her biri varsa, kabul edilebilir sınırlar içinde tutulabilir.

Yönetici sadece makul sayıda bireyden sorumludur.

ve işlevler. İşlevsel dağıtım alt sistemlere veya türlere odaklanabilir

kaynakların (örneğin medya veya programlar). İşlevsel dağılım ne zaman

yetersiz, ademi merkeziyetçilik çok önemlidir. Merkezi olmayan yönetim ile,

Her yönetici bir veya daha fazla departmandan sorumlu olabilir.

organizasyon. Özetle, erişimin etkin kontrolü,

Politika’nın, maliyet / fayda kısıtlamaları dahilinde, görevlerin ayrılması ve en az ayrıcalık ilkelerinin

onadı.

**6.10. UYGULAMA KONTROLLERİ**

Korumalı kaynak türüne erişim isteği her zaman

Bir iş veya oturumda, erişim kontrolü kararı verilmelidir. Bu karar

Yöneticilerin kaydettiği şekilde yönetimin isteklerini yerine getirmek zorundadır.

kararları veren program referans monitör olarak adlandırıldı

çünkü iş veya oturumun korumalı bir kaynağa ve

Karar referansların izlenmesi olarak görülür.

Her ne kadar referans monitörü işlevinden ziyade işlevi ile tanımlansa da

düzenlemesi, tek bir program olarak düşünmek için uygundur. Her biri için

nesnenin türü, kaynak yöneticisi adı verilen ve olması gereken bir program var.

bu tür her nesneye her erişimde yer alır. Kaynak yöneticisi

Referans monitörü, her birinin verilip verilmeyeceğini belirleyen bir hakem olarak kullanır.

koruduğu bir türdeki herhangi bir nesneye erişim istekleri kümesi.

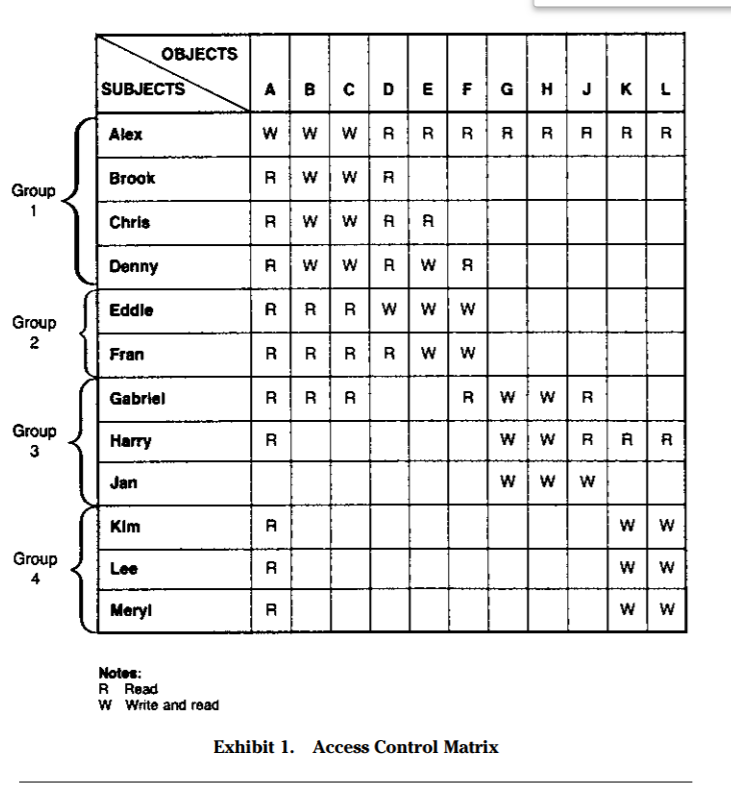
Yanıt veren bir veri tabanı yönetim sisteminde (DBMS)

tek bir alan için istekte bulunulduğunda, DBMS’nin görünüm yönetimi rutinleri

referans monitörü. Daha geleneksel olanı, bir görünüme bağlanma durumudur,

DBMS tipik olarak, kullanmak üzere iş veya oturum erişimi verilip verilmeyeceğine karar vermek için harici, çok amaçlı bir referans izleyicisi kullanır.

görünüm.



**REFERANSLAR**

**ISM: AAA 101: Key Features of an AAA Service:216**

**ISM: RADIUS: Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti:217**

**ISM: AA'yı RADIUS'a Koymak: Doğrulamalar ve Yetkiler:217**

**ISM: Üçüncü A: Eh, Bazen Yine de!:217**

**ISM: İleri Düşünme ve Diğer Gee-Whiz Yetenekleri:217**

**ISM: Tökezleyen Bloklar, Karmaşıklıklar ve Diğer RADIUS Sınırlamaları:220**

**ISM: TACACS: Terminal Erişim Kontrol Geçiş Kontrol Sistemi:220**

**ISM:A 1: TACACS Kimlik Doğrulama:221**

**ISM:A 2: TACACS Yetkilendirmesi:221**

**ISM:A 3: TACACS Muhasebe:221**

**ISM: Proksilite, Sorunlar ve Tuzaklar:221**

**ISM: ÇAP: İki kez RADIUS?:224**

**ISM: İki Brute: ÇAPETİ Yetkilendirme Yetkilendirme işlemleri:226**

**ISM: Her Şey için Muhasebe:226**

**ISM: Güvenlik, Standartlar ve Diğer Öğeler Güçlü Güvenlik Desteği:226**

**ISM: 2.Erişim Kontrollerinin Uygulanması:227**

**ISM: KATEGORİ KAYNAKLARI:227**

**ISM: Nesne Oluşturma:230**

**ISM: Veri Sınıflandırmalarını Düşürme:230**

**ISM: Etiketleme:230**

**ISM: ERİŞİM KONTROL MODELLERİ:231**

**ISM: Bell-LaPadula Modeli:232**

**ISM: Biba Modeli:232**

**ISM: Take-Grant Modeli:233**

**ISM:Clark-Wilson Modeli:233**

**ISM: Katılmamış Oturumlar:234**

**ISM:KONTROL YÖNETİMİ:236**

**ISM: Gruplandırma Konuları ve Nesneleri:236**

**ISM: Yönetici Arabirimleri:237**

**ISM: UYGULAMA KONTROLLERİ:238-239**