İşletim Sistemlerinde Dosya Dizin Kaynak Güvenliği

ISBN: 978-625-00-0260-5

Yazarlar
Hasan ZEREY
Onurcan ÇANKAYA
Ceyhan TURAN

ÖNSÖZ

Teknoloji sürekli ilerlemektedir. Kullanılan elektronik cihazlarda sürekli gelişmektedir. Gelişimin sürekli olduğu bu cihazlarda makinenin işlerliği arttıran işletim sistemleri de sürekli gelişim içerisindedir. Teknolojinin gelişimi her zaman iyi niyetli olmayabilir, art niyetli kişilerin geliştirdiği teknolojiler de hızla kendisini geliştirmektedir. Burada güvenlik kavramı karşımıza gelmektedir. Her alanda güvenlik önlemleri alınması gerektiğinden İşletim Sistemleri Güvenliği de günümüzde en önemli kavramlardan birisidir. Kullanılan platformlarda açıklıkların giderilmesi güvenli çalışma ortamları sunmaktadır.

Farklı işletim sistemlerinde bu araştırmada dosya, dizin ve kaynak güvenliği için alınması gereken önlemler sunulacaktır. Daha güvenli işletim sistemi ortamları için yapılan çalışmalar ve yapılması gereken işlemler anlatılacaktır. Basit önlemler ile işletim sistemi kullanan cihazlar için tüm kullanıcılara çözüm yolları sunacaktır.

İÇİNDEKİLER

DOSYA, DİZİN VE KAYNAK GÜVENLİĞİ

Hasan ZEREY
hasanzerey@gmail.com
Onurcan ÇANKAYA
cankayaonurcan@hotmail.com
Ceyhan TURAN

Kazanımlar

Bu bölümü tamamladıktan sonra;

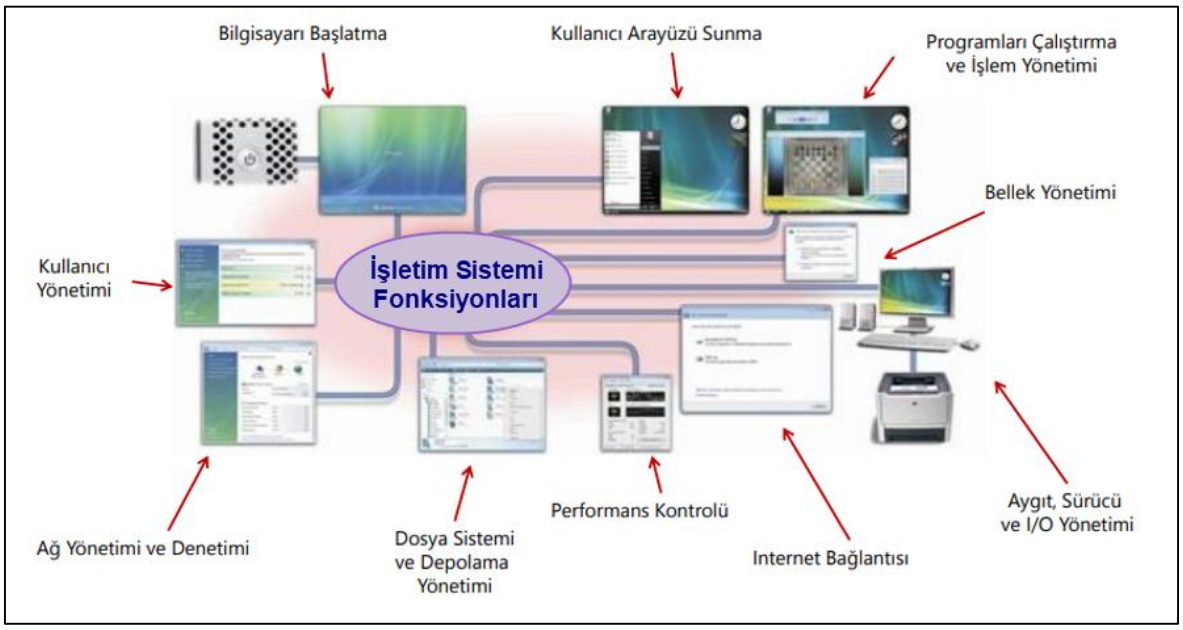
- İşletim sisteminde dosya, klasör ve kaynak güvenliğini bilir,
- Dosya sistemlerini öğrenir,
- Windows ve Linux dosya sistemi arasındaki farkları açıklayabilir,
- Dosya, dizin ve kaynak güvenliği sürecini açıklayabilir,
- Farklı işletim sistemlerini kullanarak dosya ve dizin izinlerinin nasıl uygulanabileceğini açıklayabilir,
- Ağ üzerinde güvenli dosya ve dizin paylaşımını öğrenir ve yapabilir,
- Ağ üzerinde güvenli kaynak paylaşımının nasıl olması gerektiğini öğrenir ve uygulayabilir.

İşletim Sistemleri

Bilgisayar donanımı, merkezi işlem birimi (CPU), bellek (memory), klavye ve monitör gibi giriş/çıkış birimleri (I/O Units) ile sabit disk gibi depolama birimlerinden meydana gelir. Bu bileşenler bir bilgisayarın asli işlevi olan hesaplama için gerekli olan kaynaklardır. İşletim Sistemi, bilgisayar kullanıcısı ile bilgisayar donanımı arasındaki etkileşimi sağlar (Yalçın, 2015). İşletim sistemi kullanıcıya bilgisayar kaynaklarını verimli bir şekilde kullanabilmesini sağlayan yazılım bütünüdür. Yazılım ve donanıma işlerlik kazandırarak kaynak kullanımını en üst düzeyde olmasını sağlar.

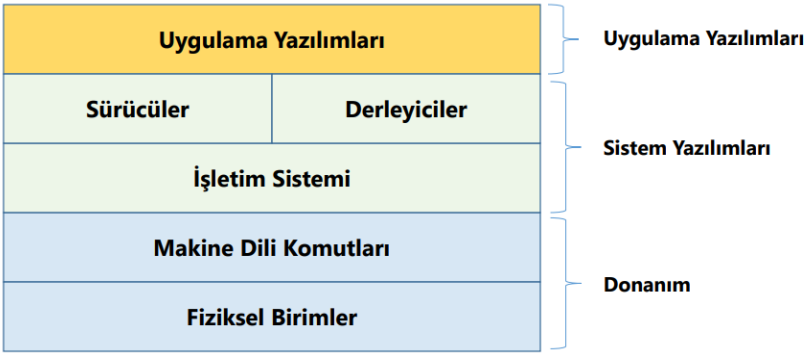
İşletim sistemleri bir bütündür. İçerisinde işlerlik sağlayan birçok küçük yapılar bulunmaktadır. Çoğu sistem küçük parçaların bir araya gelmesiyle oluşmuştur. Hücreler bir araya gelerek dokuları, dokular bir araya gelerek organları, organlar bir araya gelerek canlı organizmayı oluşturmaktadır. Canlı sistemdeki bu yapı bilgisayar sisteminde de geçerlidir. Şekil 1'de görüldüğü üzere bir işletim sisteminin fonksiyonları görülmektedir (Coşar, 2015).

Bu fonksiyonlardan biriside Dosya Sistemi ve Depolama Yönetimidir. Dosyalar İşletim sisteminin yapısı içerisinde hücreler gibidir, dosyalar ise bir anlamlı bir bütün olarak birleştiğinde ise klasör kavramına tekabül etmektedir.



Şekil 1: İşletim Sistemleri Fonksiyonları (Coşar, 2015)

İşletim sistemlerinin sundukları hizmetler farklı olmakla birlikte, aygıt yönetimi, işlem ve kaynak yönetimi, bellek yönetimi ve dosya yönetimi tüm işletim sistemlerinin sahip oldukları temel hizmetler olarak sıralanabilir (Türkoğlu, 2006). Şekil 2'de gösterildiği gibi işletim sistemi donanım katmanı ile uygulama yazılımları arasında köprü görevi göstermektedir. Dosya ve klasör yapıları yazılım bölümlerinin temel yapıtaşlarıdır.



Şekil 2: İşletim Sistemi Yapısı

Bilgisayar sisteminin gerektiği gibi kullanılması için işletim sistemi depolanan verilerin mantıksal bir görüntüsünü oluşturur. İşletim sistemi, "dosya(file)" olarak adlandırılan

mantıksal bir depolama birimi tanımlamak için, fiziksel özelliklere bağımlı değildir. İşletim sistemi, dosyaları fiziksel depolama ortamına karşılık getirir ve bu dosyalara depolama birimleri üzerinden erişmektedir (Taşcı, 2013). İşlemciler aracılığıyla günümüz bilgisayarları saniyeler içerisinde milyarlarca 1 ve 0 üzerinde işlemler yapmaktadır. Burada fiziksel katman içerisinde bilginin depolandığı birim olan sabit diskleri hızı da önemlidir. Bu araştırmada fiziksel güvenlikten ziyade yazılımsal güvenlik konusu anlatılacağı için donanımsal güvenlikten bahsedilmeyecektir.

Klasör Kavramı

Klasörler aynı yapıya ait olan dosya ve klasörlerin anlamlı bir bütün oluşturmasını sağlayan yapılardır. Örneğin resim dosyalarının karışıklık olmasın diye resimler klasörü içerisinde tutulabilir. Yine istenirse bir kişi aynı zamanlarda çekilen resimlerini yıllara ait klasörler şeklinde klasör içerisinde klasör oluşturabilir. Bu yapıya alt klasör adı verilmektedir. Klasörler ilk oluşturulduklarında boşturlar, sabit diskte belli bir alan kaplamadıkları için sonsuz sayıda oluşturulabilirler. İç içe klasör veya alt klasörler oluşturulabilir. En fazla 255 karakterlik klasör ismi verilebilir ve kelimeler arasında boşluk bırakılabilir. Klasörler tek tiptir, farklı türleri olmadığı için sadece isimleri vardır, uzantıları yoktur. Sembolleri değiştirilerek kullanılabilir.

Dosya Kavramı

Dosya, disk üzerinde depolanmış verilerin bütününe verilen isimdir. İşletim sistemi genel olarak iki çeşit dosya içerir. Birincisi, bir sistem görevi yerine getirirken ya da bir uygulama çalışırken bilgisayarı kontrol eden komutları içeren program dosyalarıdır. İkincisi ise, bir uygulama programı yardımı ile kullanıcılar tarafından yaratılmış veri dosyalarıdır.

Dosya, birbiriyle ilişkili veriler topluluğunu (bir bilgisayar programının kaynak kodu, programın derlenmiş olan çalıştırılabilir hali, metin-ses-görüntü verileri, vs.) bir saklama ünitesinde saklamak amacıyla kullanılan yapıdır (Mesut, 2016).

Dosyaların genel özellikleri şu şekildedir (Aydınalp, 2013):

- Dosyaların birer adları birer de uzantıları vardır.

- Dosya adı ile uzantısı arasında nokta (.) karakteri vardır.
- Dosya adı DOS İşletim Sisteminde en fazla 8 karakterdir, Windows İşletim Sisteminde en fazla 259 karakterdir.
- Dosya adı içerisinde özel karakter tercih edilmez. (< , >, ?, *, +, /, \, ‘ gibi)
- Dosya adı içerisinde harf, rakam veya her ikisi karışık kullanılabilir.
- DOS İşletim Sisteminde dosya adı içerisinde boşluk bırakılmaz, bunun yerine alt çizgi kullanılabilir. Windows işletim sisteminde dosya adı verilirken kelimeler arasında boşluk bırakılabilir. Arada bırakılan boşluklar da karakter sayılır.

Dosyanın adı yaptığı bir işe göre kişi ya da sistem tarafından tanımlanmaktadır. Dosya uzantısı ise hangi program ile çalıştırılacaksa ona göre bir uzantısı olur. Örneğin çalışılan dosya Word programı ile oluşturulan bir sınav dosyası ise “sınav.docx” şeklinde adlandırılır.

Dosya Sistemleri

Dosya sistemi, bir dosyanın bir disk üzerinde nasıl saklandığı ve bir bilgisayarın dosyaları yönetebilmek için erişimi nasıl sağladığını kontrol eden bir sistemdir. Farklı işletim sistemleri olduğundan her bir sistemin dosya sistemi farklıdır. Dosya sistemlerine verilebilecek örnekler:

- NTFS (New Technology File System)
- HPFS (High Performance File System)
- DOS
- FAT 16/32
- HFS (Macintosh Hierarchical File System)
- ISO 9660 (CD-ROM)
- Ext (Extended File System)

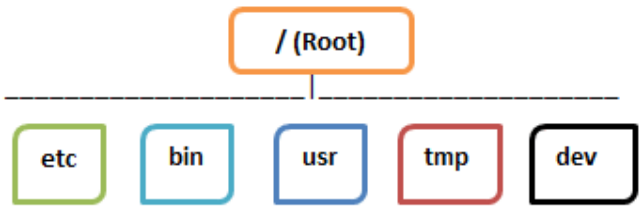
Günümüzde sıklıkla kullanılan dosya sistemleri FAT 32, NTFS dosya sistemleridir. Linux İşletim Sistemi Ext2, Ext3 ve Linux Swap dosya sistemlerini kullanır. MS-DOS işletim sistemi FAT 16, Windows 95/98 işletim sistemi FAT 32, Windows NT/2000/XP/Vista/7/8/10 işletim sistemleri NTFS, OS/2 işletim sistemi HPFS dosya sistemlerini kullanmaktadır (Kurt, 2005). Tablo 1’de farklı dosya tiplerinin karşılaştırılması verilmiştir.

Features	NTFS	FAT32	FAT16	FAT12
Max Partition Size	2TB	32GB	4GB	16MB
Max File Size	16TB	4GB	2GB	Less than 16MB
Cluster Size	4KB	4KB to 32KB	2KB to 64KB	0.5KB to 4KB
Fault Tolerance	Auto Repair	No	No	No
Compression	Yes	No	No	No
Security	Local and Network	Only Network	Only Network	Only Network
Compatibility	Windows 10/8/7/XP/Vista/2000	Windows ME/2000/XP/7/8.1	Windows ME/2000/XP/7/8.1	Windows ME/2000/XP/7/8.1

Tablo 1: Dosya Sistemlerinin Karşılaştırılması

Microsoft ve Windows farklı dosya sistemleri kullanılmaktadır. Microsoft Windows'ta dosyalar, C: D: E gibi farklı veri sürücülerindeki klasörlerde depolanır. Bilgisayarda veri kavramı, bir işlem tarafından kendisini kullanıp işi bittikten sonra da varlığını devam ettirmek zorundadır. Bu sistem sayesinde oldukça büyük miktarda verileri depolamak mümkündür. Yine bu sayede, çoklu işlemler verilere eş zamanlı olarak erişebilmektedir. Çözüm, bu verileri disk veya diğer medyalara üniteler halinde saklamaktır (Samet, 2018).

Ancak, Linux'ta dosyalar, kök dizin ile başlayan bir ağaç yapısında sıralanır. Bu kök dizin, dosya sisteminin başlangıcı olarak düşünülebilir ve ayrıca çeşitli diğer alt dizinleri de dallandırır. Kök, eğik çizgi '/' ile gösterilir. Linux dosya yapısı Şekil 3'de gösterilmiştir. Kök dizin "Root" olarak tanımlanmaktadır.



Şekil 3: Linux Dosya Yapısı

Linux işletim sisteminde kullanılan alt dizinlerin işlevleri Tablo 2'de verilmiştir.

Dizin	Açıklama
/bin	Sistemi başlatmak ve diğer önemli sistem görevlerini gerçekleştirmek için gerekli programlar olan ikili dosyalar veya çalıştırılabilir dosyalar içerir; ayrıca dizin, tüm kullanıcıların UNIX ve Linux ile çalışması gereken birçok programı barındırır
/boot	Önyükleme yükleyicisinin (işletim sistemini başlatan yardımcı program) ihtiyaç duyduğu dosyaları içerir; ayrıca çekirdek (işletim sistemi) görüntülerini içerir
/dev	Sabit diskler, fare, yazıcılar, konsollar, modemler, bellek, disketler ve CD-ROM sürücüsü gibi sistem aygıtlarına ve kaynaklarına başvuran dosyalar içerir
/etc	Sistem açısından kritik bilgiler içerdikleri için çoğu sistem yöneticisine ayrılmış olan, bilgisayar başlatıldığında sistemin kullandığı yapılandırma dosyalarını içerir.
/lib	Programcıların programlarında bu kodun kopyalarını oluşturmak yerine genellikle kütüphanelerde kod paylaşmak için kullandıkları dosyalar olan çekirdek modüllerini, güvenlik bilgilerini ve paylaşılan kütüphane görüntülerini içerir
/mnt	Sistem yöneticisi tarafından bir CD-ROM sürücüsünün takılması gibi geçici bağlamalar için bağlama noktaları içerir
/proc	Yalnızca belleğe ayrılmış ve sistem üzerinde çalışan çeşitli işlemlere atıfta bulunan dosyaların yanı sıra işletim sistemi çekirdeği ile ilgili ayrıntıları içeren sanal bir dosya sistemi
/root	Kök kullanıcı için ana sayfa
/sbin	Sistemi başlatan programları, dosya sistemi onarımı için gerekli programları ve temel ağ programlarını içerir; sadece yönetici tarafından erişilir
/var	Performans ve hata günlükleri gibi sık değişen dosyaları içerir

Tablo 2: Linux Alt Dizinlerin İşlevleri

Windows ve Linux Dosya Sistemi Farklar

Windows ve Linux İşletim sistemleri arasındaki farklar aşağıda sıralanmıştır:

- Uzantılar dosya hakkında bir takım bilgiler içerir. Bazı işletim sistemleri için ise uzantı önemli değildir. UNIX ve Linux dosya uzantılarını dikkate almazlar. Fakat bazı uygulamalar uzantılara bağlı olarak çalışabilir.

- Linux, açık kaynaklı bir işletim sistemidir, böylece kullanıcı, kaynak kodunu gereksinime göre değiştirebilir, oysa Windows işletim sistemi ticari bir işletim sistemidir, bu nedenle kullanıcının kaynak koda erişimi yoktur.
- Linux, hataları tespit etmek ve düzeltmek kolay olduğu için oldukça güvenlidir, oysa Windows büyük bir kullanıcı tabanına sahiptir, bu nedenle bilgisayar korsanlarının Windows sistemine saldırması hedefi haline gelir.
- Linux, eski donanımlarla bile daha hızlı çalışır, oysa Windows Linux'a kıyasla daha yavaştır.
- Sabit sürücüler, CD-ROM'lar, yazıcılar gibi Linux çevre birimleri dosya olarak kabul edilirken, Windows, sabit sürücüler, CD-ROM'lar, yazıcılar aygıt olarak kabul edilir.
- Linux dosyaları, kök dizinden başlayarak bir ağaç yapısında sıralanır, oysa Windows'ta dosyalar C: D: E gibi farklı veri sürücülerindeki klasörlerde depolanır.
- Linux'ta aynı dizinde aynı ada sahip 2 dosya olabilirken, Windows'ta aynı klasörde aynı ada sahip 2 dosya bulunamaz.
- Linux'ta sistem ve program dosyalarını farklı dizinlerde bulabilirsiniz, oysa Windows'ta sistem ve program dosyaları genellikle C: sürücüsüne kaydedilir.
- Linux ve UNIX'te her şey bir dosyadır. Dizinler dosyalardır, dosyalar dosyalardır ve Yazıcı, fare, klavye vb. Aygıtlar dosyalardır.

Erişim Kontrol Listeleri

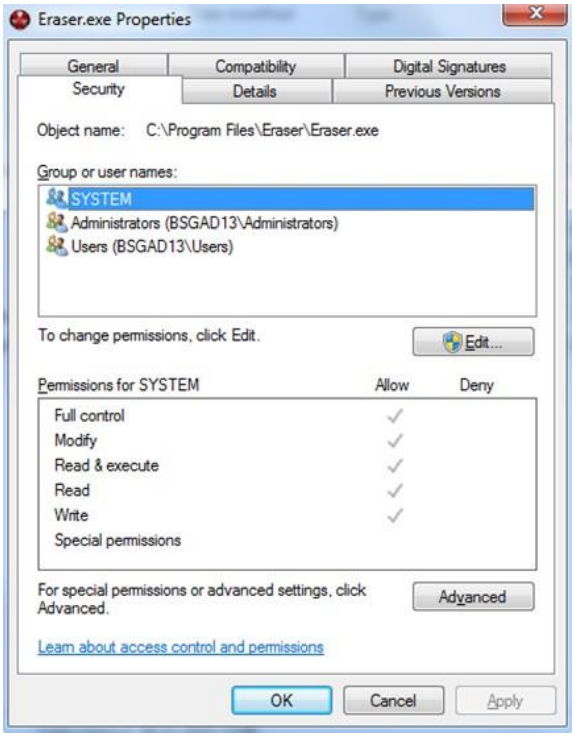
Erişim kontrol listeleri (Access Control List – ACL), kullanıcıları ve grupları belirli erişim yetenekleriyle ilişkilendirir. ACL, erişim Kontrol Kayıtları'nın (Access Control Entry – ACE) değerlerinin bir araya gelmesi ile oluşurlar. ACL içerisindeki her bir ACE nesnesi bir kullanıcı ya da grubuna erişim hakkı vermede, erişimi engellemede veya erişim denetiminde kullanılır. DACL ve SACL olmak üzere iki türde ACL vardır (Başaranoğlu, 2015).

a) İsteğe Bağlı Erişim Kontrol Listesi (Discretionary Access Control List - DACL)

Korunabilen bir nesneye bir kullanıcının veya grubun erişimine izin vermede ya da engellemede kullanılır. Bir işlem, bir nesneye erişmeye çalıştığında gerekli izninin olup olmadığı DACL içinde bulunan ACE nesneleri sistem tarafından kontrol edilerek belirlenir. Eğer bir nesne üzerinde herhangi bir DACL bulunmuyorsa, sistem bu nesne üzerinde tüm

kullanıcılara tam kontrol (full control) izni verir. Eğer nesnenin DACL değerinde herhangi bir ACE nesnesi bulunmuyorsa, sistem nesneye erişmeye çalışan tüm denemeleri engelleyecektir. Çünkü DACL, herhangi bir ACE bulundurmadığı için herhangi bir erişim hakkı da söz konusu olamayacaktır. Sistem nesne erişimlerinde, erişilmeye çalışılan nesnenin DACL'inde erişime izin veren herhangi bir ACE nesnesini bulana kadar aramaya devam edecektir, böyle bir nesne bulamazsa nesne erişimine izin verilmeyecektir (Başaranoğlu, 2015). Windows işletim sisteminde DACL yapısı Şekil 4'de gösterilmiştir. ACL'deki bilgi kategorileri;

- Nesneye erişebilen kullanıcı hesapları
- Erişim düzeyini belirleyen haklar ve izinler
- Nesnenin sahipliği
- Bir nesneyle ilişkili belirli olayların denetlenip denetlenmeyeceği



Şekil 4: DACL Yapısı

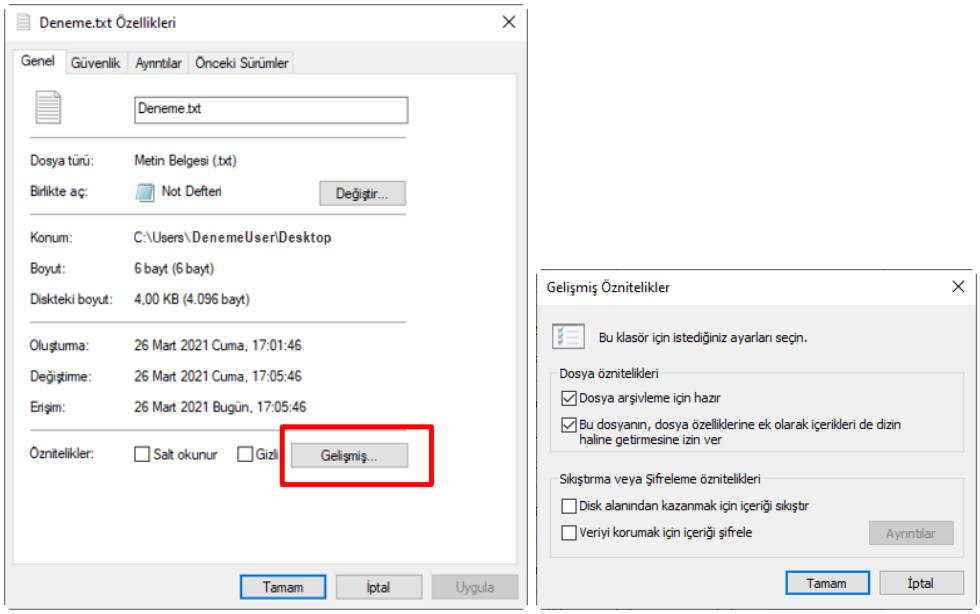
b) Sistem Erişim Kontrol Listesi (System Access Control List - SACL)

System Access Control List (SACL) ise korunabilen bir nesneye erişme girişiminde bulunan tüm girişimlerin kayıt bilgisinin tutulmasında kullanılır. Her bir ACE nesnesi burada erişilmeye çalışılan nesne için hangi kullanıcı veya grubun hangi erişim türü için (başarılı – başarısız) güvenlik kayıt bilgileri (security event log) ekranına kayıt girileceğini tanımlamada kullanılır. SACL ile başarılı, başarısız ya da her iki durum için de kayıt bilgisi üretilmesi sağlanabilir (Başaranoğlu, 2015). . Windows işletim sisteminde sACL yapısı Şekil 5'de gösterilmiştir.

Şekil 5: SACL Yapısı

Dosya Güvenliği

Windows ortamında bir dosyanın güvenlik yapılandırılması pencereler aracılığıyla yapılmaktadır. Dosya ile ilgili güvenlik ayarları için, ilgili dosyanın üzerinde Mouse ile sağ tuş tıklanır. Gelen menü seçeneklerinden "özellikler" seçildiğinde Şekil 6 penceresi ekrana gelmektedir. Gelişmiş seçeneklerinde ise daha farklı seçenekler görüntülenmektedir.



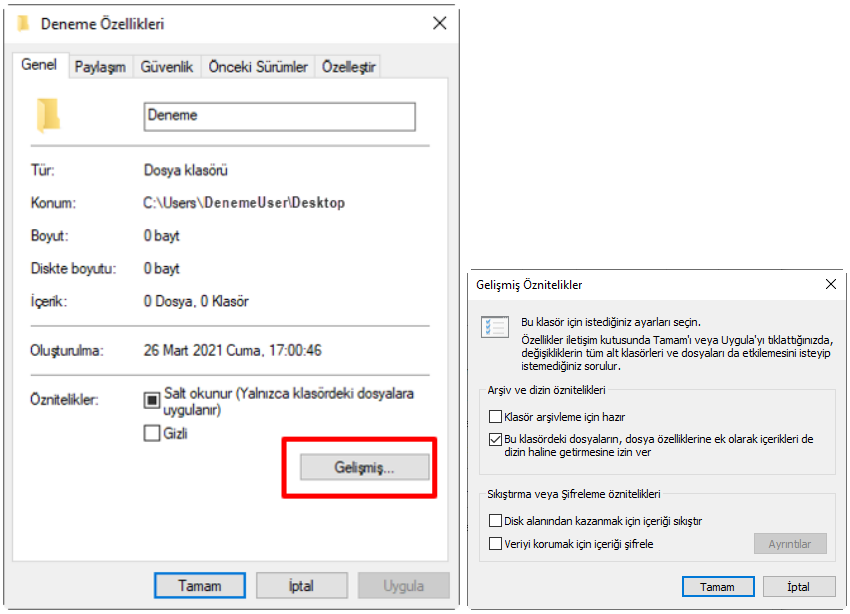
Şekil 6: Dosya özellikleri ve Gelişmiş Penceresi

Bu özelliklerden bazıları:

- **Salt okunur:** Bu izin bir dosya sadece okuma imkânı verir, ancak dosyaya herhangi bir şey yazmak veya içeriğini değiştirmek mümkün değildir.
- **Gizli:** Bu özellik ile komut isteminde normal bir dizin oluştururken dosya gösterilmeyecektir. Genellikle sistem dosyaları gizli olmakla birlikte, siz de acemi kullanıcılara karşı, önemli dosyalarınızın gözlerden uzak olmasını sağlar.
- **Gelişmiş:** Bu düğmeye tıklanarak, dosyaların arşiv niteliği ve şifreleme özellikleri değiştirilebilir.

Dizin (Klasör) Güvenliği

Windows ortamında bir klasörün güvenlik yapılandırılması dosyalar seçeneğinde olduğu gibi pencereler aracılığıyla yapılmaktadır. Klasör ile ilgili güvenlik ayarları için, ilgili klasörün üzerinde Mouse ile sağ tuş tıklanır. Gelen menü seçeneklerinden “özellikler” seçildiğinde Şekil 7 penceresi ekrana gelmektedir. Gelişmiş seçeneklerinde ise daha farklı seçenekler görüntülenmektedir.



Şekil 7: Klasör özellikleri ve Gelişmiş Penceresi

Bu gelişmiş özelliklerin açıklamaları:

- **Arşiv ve dizin öznitelikleri:** Bu izin bölümü bir klasörün arşivleme için hazır hale getirilmesini sağlar. Aynı zamanda bu klasörün içerisindeki dosya ve alt klasörlerin de özelliklerinin de arşivlemeye hazır hale getirilmesini sağlamaktadır.
- **Sıkıştırma ve Şifreleme öznitelikleri:** Dosya şifreleme, verilerinizi şifreleyerek korumanıza yardımcı olur. Sadece doğru şifreleme anahtarı (parola gibi) olan bir kişi bu şifreyi çözebilir.

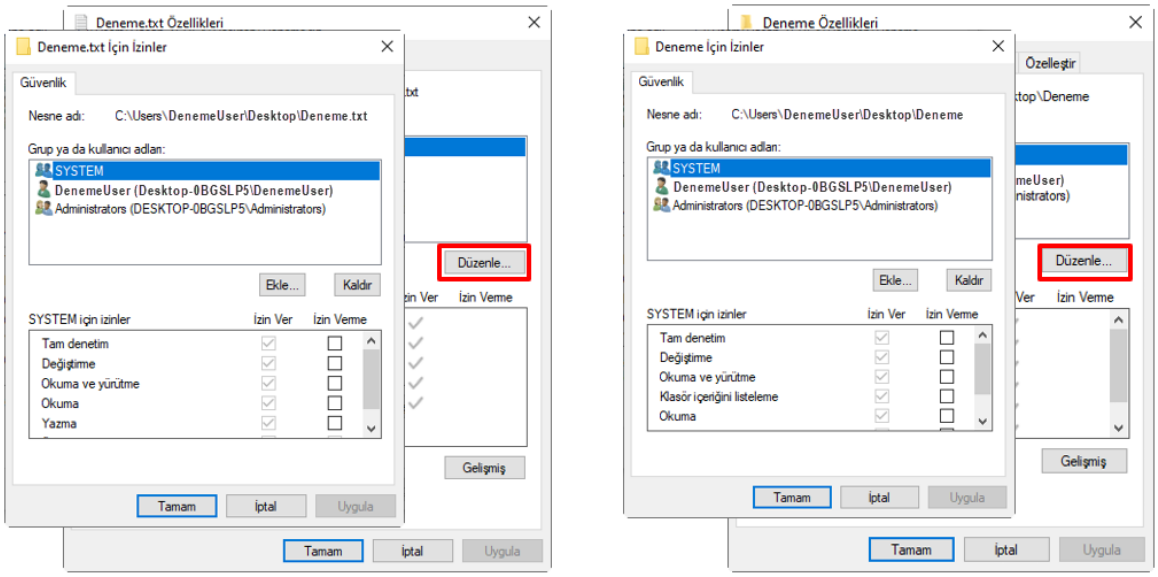
Linux işletim sistemleri, dosya özniteliklerini ayarlamak için chattr (Change Attribute) komutunu kullanabilirken, Mac OS X'te chflags (Change Flags) kullanılır.

Dosya, Dizin Paylaşım Güvenliği

Farklı işletim sistemlerinde dosya ve dizin paylaşım güvenliği ayarları bu bölümde sunulacaktır.

a) Windows İşletim Sistemi Dosya, Dizin Paylaşım Güvenliği

Windows işletim sisteminde hangi kullanıcıların ve grupların izne sahip olduğunu değiştirmek için Şekil 8'de klasör özellikleri Güvenlik sekmesindeki "Ekle ve Kaldır" düğmelerini kullanılmalıdır. Gruba tıklayarak, "İzin Ver" ve "İzin Verme" sütunlarındaki kontrolleri kontrol ederek veya kaldırarak mevcut izinleri değiştirmek gerekmektedir. Bu şekilde güvenlik ilkesi oluşturarak dosya ve klasör güvenlik politikası oluşturmak mümkündür.



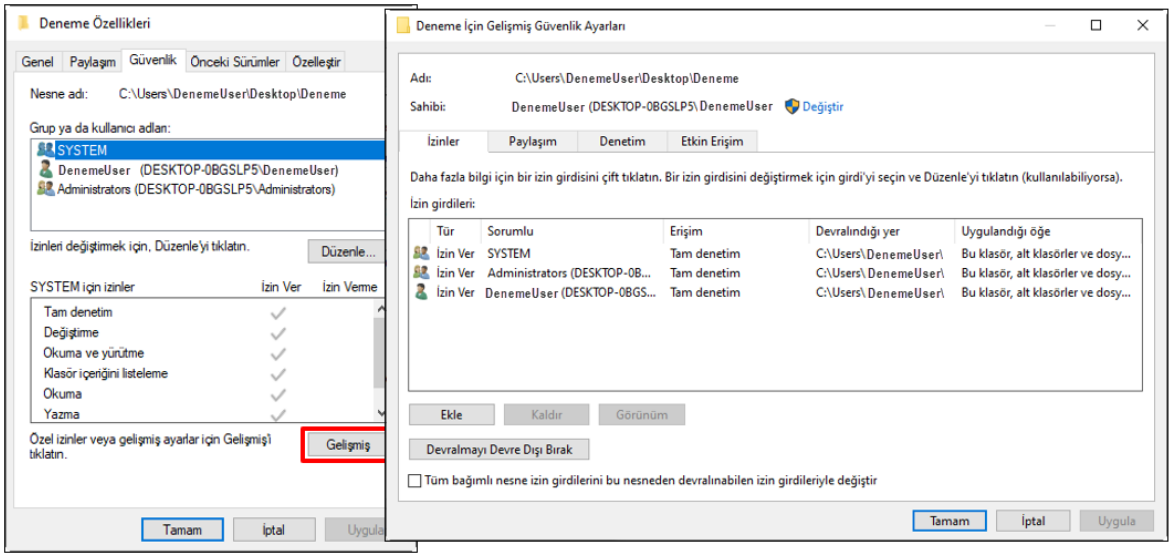
Şekil 8: Dosya ve Dizin Güvenlik Ayarları Penceresi

Bu bölümde yer alan bölümlerde hangi tanımlamalara izin verilip verilmeyeceği ayarlanmaktadır. Bu tanımlamaların açıklamaları Tablo 3'de verilmiştir.

İzin	Açıklama	Geçerliliği
Tam Denetim	Dosyaları okuyabilir, ekleyebilir, silebilir, yürütebilir ve değiştirebilir, ayrıca izinleri ve öznitelikleri değiştirebilir ve sahiplik alabilir	Klasörler ve dosyalar
Klasör içeriğini listeleme	Klasördeki dosyaları listeleyebilir (geçiş yapabilir) veya bir alt klasöre geçebilir, klasör özniteliklerini ve izinleri görüntüleyebilir ve dosyaları yürütebilir, ancak dosya içeriklerini görüntüleyemez	Yalnızca klasörler
Değiştirme	Dosyaları okuyabilir, ekleyebilir, silebilir, yürütebilir ve değiştirebilir, ancak alt klasörleri ve dosya içeriklerini silemez, izinleri değiştiremez veya sahiplik alamaz	Klasörler ve dosyalar
Okuma	Dosya içeriğini görüntüleyebilir ve klasör özniteliklerini ve izinlerini görüntüleyebilir, ancak klasörler arasında geçiş yapamaz veya dosyaları yürütemez	Klasörler ve dosyalar
Oku ve Yürütme	Hem Klasör İçeriklerini Listeleme hem de Okuma (klasörleri dolaşma, dosya içeriklerini görüntüleme, öznitelikleri ve izinleri görüntüleme ve dosyaları yürütme) yeteneklerini içerir	Klasörler ve dosyalar
Yazma	Dosya oluşturabilir, dosyalara veri yazabilir, dosyalara veri ekleyebilir, klasörler oluşturabilir, dosyaları silebilir (ancak alt klasörleri ve dosyalarını değil) ve klasör ve dosya özniteliklerini değiştirebilir	Klasörler ve dosyalar

Tablo 3: Dosya ve Dizin Güvenlik Seçenekleri

Windows ortamında yapılacak bir diğer ayarlama ise Şekil 9'da gösterildiği gibi gelişmiş seçenekler gösterilmektedir. Bu bölümde verilen izinlerin özet olarak gösterildiği bölümdür. Daha fazla bilgi alabilmek için pencereden dosya veya klasörün farklı kullanıcılardaki izinleri ayarlanabilir. Paylaşım olarak hangi ağlarda paylaşıldığını görüntülemekte mümkündür. Denetim yetkisinin hangi kullanıcılarda olduğu ve etkin erişim olarak yetkinin kimlerde olduğu görüntülenmektedir.



Şekil 9: Dosya ve Dizin Gelişmiş Güvenlik Ayarları Penceresi

b) Linux, Unix İşletim Sistemi Dosya, Dizin Paylaşım Güvenliği

Dosya ve dizin güvenlik ayarları ile ilgili olarak farklı işletim sistemlerindeki kullanımlarından bahsedelim. Linux ve Unix işletim sistemlerinde 3 grup bulunmaktadır:

- Owner (Sahip)
- Group (Grup)
- Other users (Diğer Kullanıcılar)

Bazı kaynaklarda bir kullanıcı daha olduğundan bahsedilmektedir. Aslında dördüncü grup tüm gruplar olarak geçmektedir. İzinler olarak ise;

- Okuma (r)
- Yazma (w)
- Yürütme (x)

Okuma hakkı, bir dosyayı okumak yetkisidir. Yazma hakkı, bir dosyayı yaratmak ve istendiğinde dosyayı değiştirmek ya da silmek yetkisidir. Execute (çalıştırma) hakkı, bir dosyayı çalıştırma, kullanma yetkisidir. Linux ve Unix işletim sistemleri çok kullanıcılı bir sistem olduğu için, her kullanıcı ancak kendisine erişim izni verilen dosyalara erişebilir ve dosya ile ilgili olarak yapabileceği işler, kendisine verilen erişim hakkıyla sınırlıdır. Böyle olmasaydı, bir kullanıcı başka bir kullanıcının dosyalarını okuyabilir, üzerinde istenmeyen değişiklikler yapabilir ve hatta silebilirdi. Bu durum güvenlik ilkelerinin esnemesine neden olabilir. Çalıştırılabilir programlar için özel izinler ise şunlardır;

- Kullanıcı Kimliğini (SUID) Ayarla
- Grup Kimliğini (SGID) Ayarla

Burada da grup ilkelerini tanımlama yapma imkânı bulunmaktadır. Sistemin verimliliği açısından bu ilkeler çok önemlidir. Bir dosyanın özniteliklerinin ayrıntılarını **ls** komutunu –**l** anahtarıyla (örneğin **ls –l dosya adı**) listelerseniz, komut **-rwe-rw-r** gibi görünen bilgileri döndürür ve bu da okuma, yazma ve sahip için ayrıcalıkları yürütme, grup için okuma ve yazma ayrıcalıkları ve diğer tüm kullanıcılar için yalnızca okuma erişimi bulunmaktadır. Erişim hakkı türlerinin her biri, aşağıda listelenen ilişkili bir sayısal değere sahiptir (Bradley, 2020):

- Oku = 4
- Yazma = 2
- Yürütme = 1

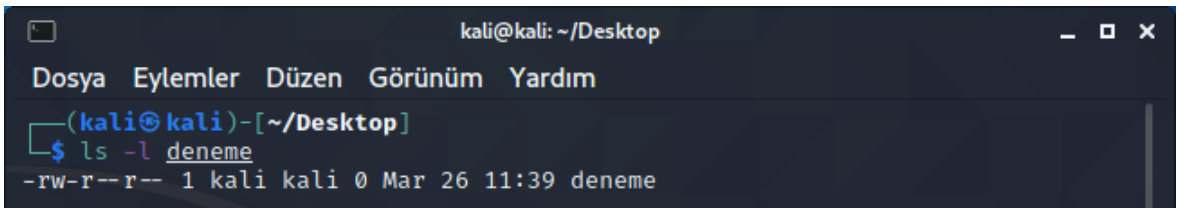
Değerlerini chmod (mod değiştir) komutunu kullanarak izinleri atamak veya değiştirmek için kullanılabilen, 0 ile 7 arasında bir değer elde etmek için toplanır. Söz konusu dosya için erişim hakları

chmod 764 dosya adı

Girilerek atanabilir. 764 sayısı şunlardan türetilmiştir:

- owner : rwe = 4 (oku) + 2 (yaz) + 1 (çalıştır) = 7
- group : rw = 4 (okuma) + 2 (yazma) = 6
- diğerleri : r = 4 (okuma) = 4 şeklinde hesaplanarak bulunmuştur.

Bu konuyla ilgili kali Linux ortamında bir uyguluma sunulacaktır. Masaüstü ortamında "deneme" isimli bir dosya oluşturulmuştur. Terminal ekranı açılarak ls –l komutu kullanarak listeleme şu şekilde gerçekleştirilir;



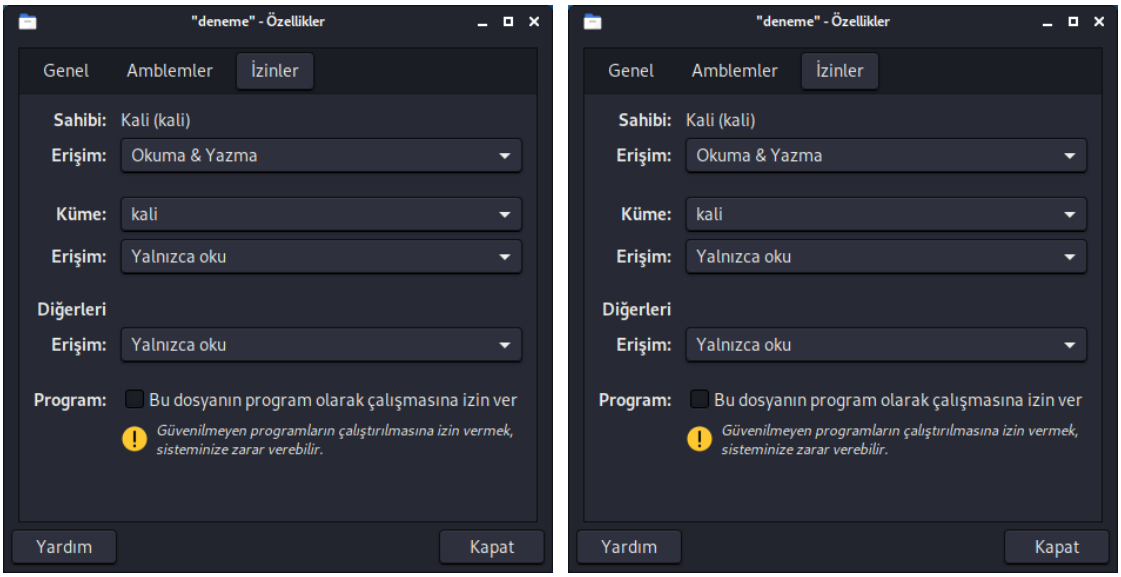
Görüldüğü üzere oluşturulan dosyanın kullanım izinleri listelenmiş oldu. -rw-r--r-- sonucu ile sahip okuma ve yazma, grup ve diğerlerinde sadece okuma yetkisi olduğu görülmüştür. Yukarıda bahsedilen 0 ile 7 arasında okuma, yazma ve çalıştırma yetkilerinin ayarlanması için chmod komutu şu şekilde kullanılmalıdır.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 764 deneme
```

Bu şekilde kullanım izinleri değiştirilmiş olundu. Tekrar terminal ekranında listeleme komutu uygulandığında;

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l deneme
-rwxrw-r-- 1 kali kali 0 Mar 26 11:39 deneme
```

Sonucu alınmaktadır. Terminal ekranındaki görünüm bu şekildeydi. Yine Linux ekranında deneme isimli dosyanın üzerinde sağ tuş yaparak özellikler seçeneği Şekil 10'da gösterilmiştir. Yine bu ekranda komutları çalıştırmadan önceki hali ve sonrası da verilmiştir.

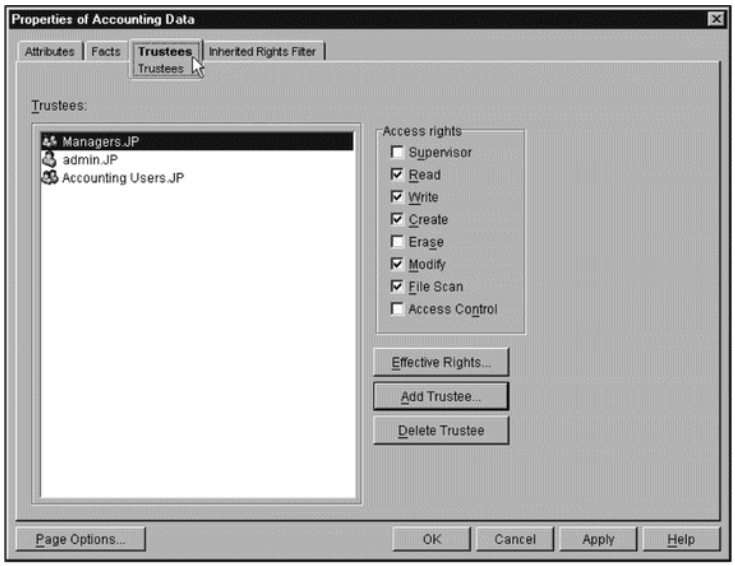


Şekil 10: chmod Komutu Öncesi ve Sonrası Pencere Görünümü

c) Netware İşletim Sistemi Dosya, Dizin Paylaşım Güvenliği

Netware işletim sisteminde Şekil 11'de pencere yapısı görüntülenmektedir. Netware işletim sistemin dosya ve dizin paylaşım güvenliği erişimi için şu şekilde kontrol edilir:

- Dosya ve dizinlerle ilişkili öznitelikler
- Mütevellilere verilen erişim hakları



Şekil 11: Netware İşletim Sistemi Pencere Görünümü

Şekil 11'de pencere üzerinde bulunan seçeneklerin açıklaması

Dizin	Açıklama
/bin	Sistemi başlatmak ve diğer önemli sistem görevlerini gerçekleştirmek için gerekli programlar olan ikili dosyalar veya çalıştırılabilir dosyalar içerir; ayrıca dizin, tüm kullanıcıların UNIX ve Linux ile çalışması gereken birçok programı barındırır
/boot	Önyükleme yükleyicisinin (işletim sistemini başlatan yardımcı program) ihtiyaç duyduğu dosyaları içerir; ayrıca çekirdek (işletim sistemi) görüntülerini içerir
/dev	Sabit diskler, fare, yazıcılar, konsollar, modemler, bellek, disketler ve CD-ROM sürücüsü gibi sistem aygıtlarına ve kaynaklarına başvuran dosyalar içerir
/etc	Sistem açısından kritik bilgiler içerdikleri için çoğu sistem yöneticisine ayrılmış olan, bilgisayar başlatıldığında sistemin kullandığı yapılandırma dosyalarını içerir.
/lib	Programcıların programlarında bu kodun kopyalarını oluşturmak yerine genellikle kütüphanelerde kod paylaşmak için kullandıkları dosyalar olan çekirdek modüllerini, güvenlik bilgilerini ve paylaşılan kütüphane görüntülerini içerir
/mnt	Sistem yöneticisi tarafından bir CD-ROM sürücüsünün takılması gibi geçici bağlamalar için bağlama noktaları içerir
/proc	Yalnızca belleğe ayrılmış ve sistem üzerinde çalışan çeşitli işlemlere atıfta bulunan dosyaların yanı sıra işletim sistemi çekirdeği ile ilgili ayrıntıları içeren sanal bir dosya sistemi
/root	Kök kullanıcı için ana sayfa
/sbin	Sistemi başlatan programları, dosya sistemi onarımı için gerekli programları ve temel ağ programlarını içerir; sadece yönetici tarafından erişilir
/var	Performans ve hata günlükleri gibi sık değişen dosyaları içerir

Tablo 4: Netware İşletim Sistemi Pencere Seçenekleri

d) MAC İşletim Sistemi Dosya, Dizin Paylaşım Güvenliği

Macintosh İşletim Sisteminde (MAC OS) bir dosya ve klasörün üzerinde kullanım ayarları ekranının bir kesiti Şekil 12'de sunulmuştur. MAC OS'da dosya ve klasör izinlerini yapılandırma yolları;

- Komut satırı komutları
- Bir dosyanın ya da klasörün Bilgi Alma özellikleri seçenekleri kullanılmaktadır.

Şekil 12: MAC İşletim Sistemi Pencere Görünümü (Apple, t.y.)

Pencere üzerinde bulunan seçeneklerin açıklamaları tablo 5'de verilmiştir. Linux benzeri bir yapı söz konusudur. Grup ilkelerine yetkiler verilmesi söz konusudur.

İzinler	Açıklama
Read & Write	Bir klasörün içeriğini görüntüleyebilir, o klasöre dosya ekleyebilir veya silebilir ve programları çalıştırabilir; dosyalar için, dosya içeriğini okuyabilir, dosyaları değiştirebilir, dosyaları silebilir ve bir program dosyasını çalıştırabilir
Read only	Bir klasör veya dosyanın içeriğini görüntüleyebilir ve bir klasördeki bir programı çalıştırabilir; dosyalar için, dosyanın içeriğini okuyabilir ve bir program dosyasını çalıştırabilir
Write only (Drop Box)	Yalnızca bir klasör için, kullanıcının klasör içeriğini o kullanıcının ana dizininin Genel klasöründeki DropBox klasörüne kopyalamasını sağlar.
No Access	Bir klasöre veya dosyaya erişilemiyor

Tablo 5: MAC İşletim Sistemi Pencere Seçenekleri

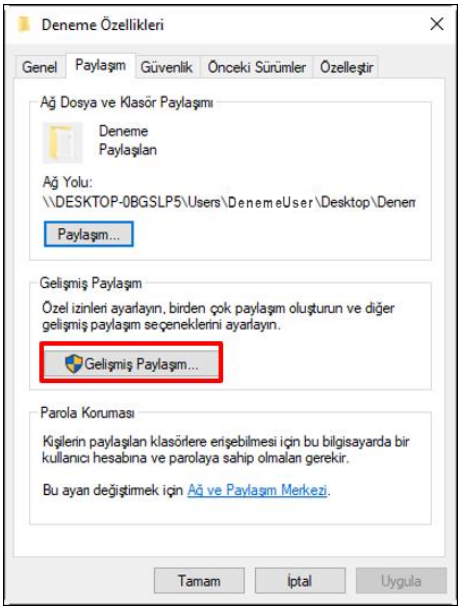
Paylaşılan Kaynak Güvenliği

İşletim Sistemlerinde kaynak paylaşımı önemli bir konudur. Bilgisayar yapısında sınırsız kaynak mümkün değildir. Ama kaynakların paylaşımı kaynakların genişletilmesini ve arttırılmasını sağlamaktadır. Bir ağ üzerinden kaynakları - dizinler, klasörler, dosyalar ve yazıcılar - paylaşma veya bunlara erişme izinlerini kapsar.

a) Ağ Üzerinde Dosya, Dizin Paylaşım Güvenliği

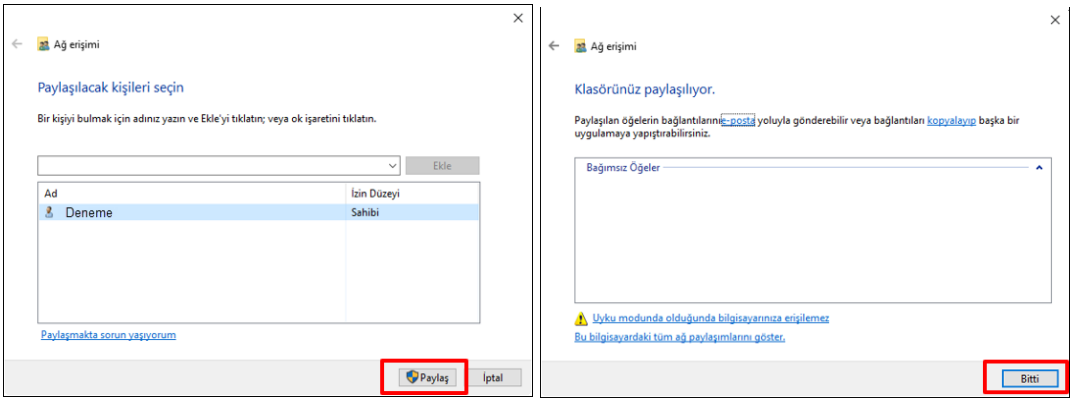
Ağ üzerinde erişimde esas olan güvenlik önlemi izinlerdir. Paylaşımda dosya veya klasörler yerel olarak paylaşılacaksa paylaşım ayarlarında gerekli yetkilerin verilmiş olması gerekmektedir. Burada kaynak paylaşımı yapılacaksa sistem sürücüsü gibi kritik sürücülerin tam erişimi verilmemelidir. Sistem üzerinde büyük açık kapılar bırakmak sistemin sürdürülebilirliği açısından büyük sıkıntılara neden olabilir. Bu sebepten paylaşılacak belirli bir kaynak ve belirli kişiler belirlemek her zaman sistem açısından önemlidir.

Windows işletim sistemi üzerinde Şekil 13'de deneme isimli klasörün özellikler penceresi görülmektedir. Pencerede Paylaşım sekmesi açılır. Burada yine Paylaşım butonu işaretlenerek paylaşım ayarları yapılmaya başlanılır (Boyan, 2020).



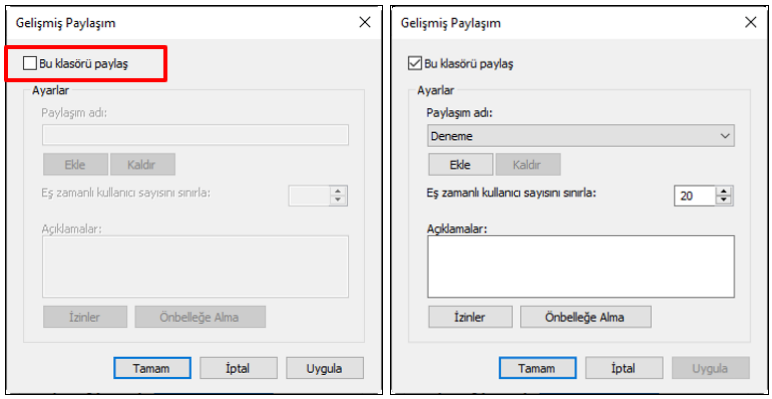
Şekil 13: Klasör Özellikleri Penceresi

Daha sonrası Şekil 14'de paylaşılacak ağ kullanıcıları aranmalıdır. Paylaşımda yetki verilecek kullanıcı ağ üzerinde bulunduktan sonra paylaş butonuna basılır. Bir sonraki ekranda ise paylaşılacak kişiler özet olarak tekrar gösterilmektedir. Herhangi bir yanlış paylaşım yapılmaması adına burada dikkat edilmelidir. Bitti butonuna basılarak paylaşılacak kullanıcı belirlenmiş oldu (nongraper, 2019).



Şekil 14: Ağ Erişim Kullanıcı Ekleme

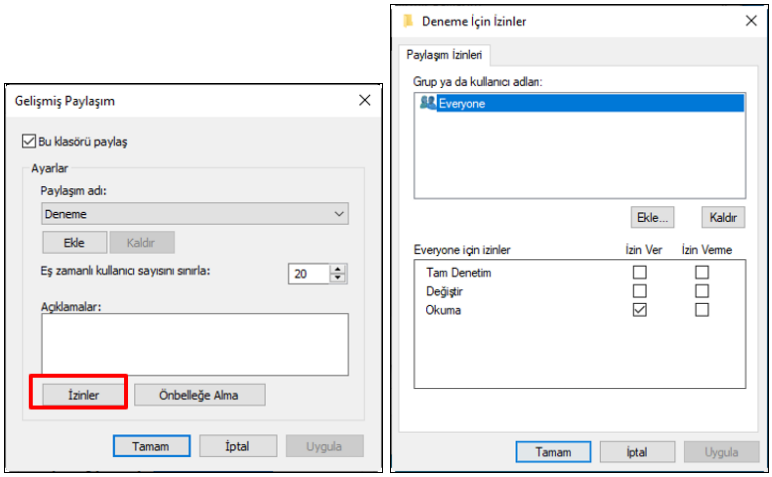
Paylaşılan kullanıcının güvenlik açısından yetkilerinin düzenlenmesi gerekmektedir. Şekil 13'deki pencere "Gelişmiş Paylaşım…" butonuna basılmalıdır. Gelen pencereden "Bu klasörü paylaş" onay kutusu seçilmelidir. Seçim yapıldıktan sonra Paylaşım adı bölümü aktif hale gelecektir.



Şekil 15: Gelişmiş Paylaşım Pencereleri

Buraya kadar yapılan işlemlerde herhangi bir kısıtlama verilmediği görülmektedir. Bu aşamada yetki kısıtlaması eklenecektir. Şekil 15'deki ekranda paylaşım sonrası "İzinler" butonu aktif hale gelmiştir. Şekil 16'da görüldüğü gibi tıklandığında Deneme klasörü için izinler penceresi ekrana gelir. Bu ekranda "Everyone" seçiliyse ağda olan herhangi bir kullanıcıdan bahseder. Ağa bağlı olan herhangi birine yetki vermek güvenlik açısından problemdir. Verilen yetkide belirlenen kullanıcı seçilmelidir. Paylaşılan klasörün içerisinde örneğin bir metin dosyası olduğu farz edelim. Bu dosyada tam izin verilirse isterse okuyabilir, değiştirebilir veya silebilir. Dosyanın güvenliği açısından bu da problem olabilir. Değiştir seçilirse okuyup içeriği değiştirebilir. Okuma seçiliyse sadece dosyanın içeriğine

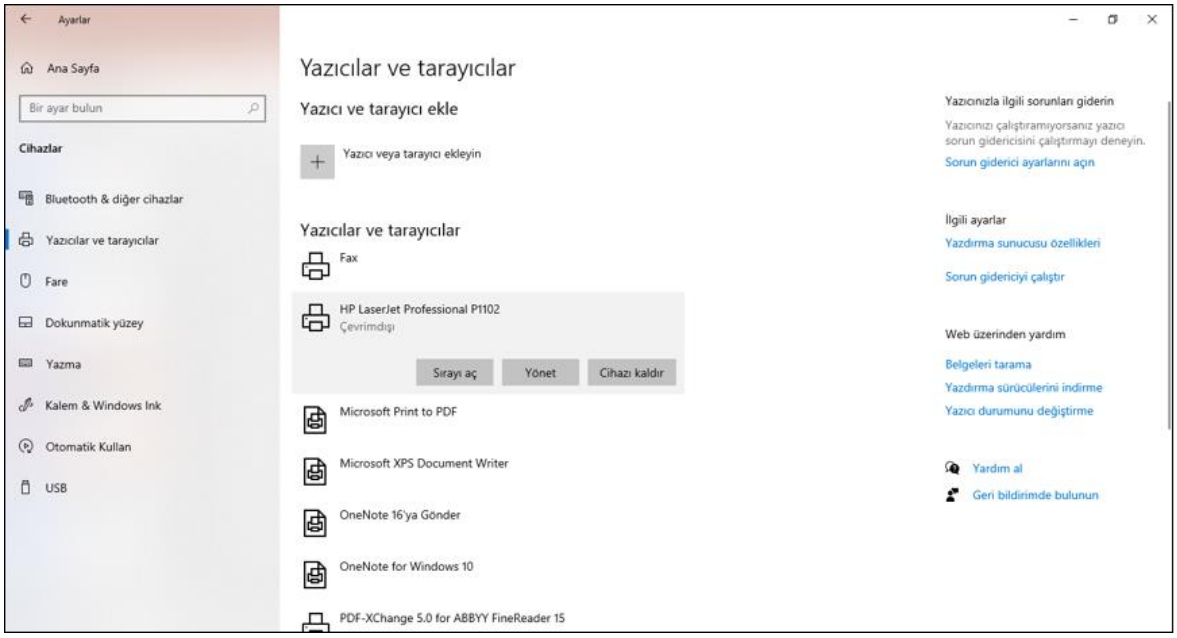
bakabilir, silemez ve değiştiremez. Bu bakımdan kullanıcıya verilen izinler işletim sistemi açısından çok önemlidir.



Şekil 16: Gelişmiş Paylaşım İzinleri Pencereleri

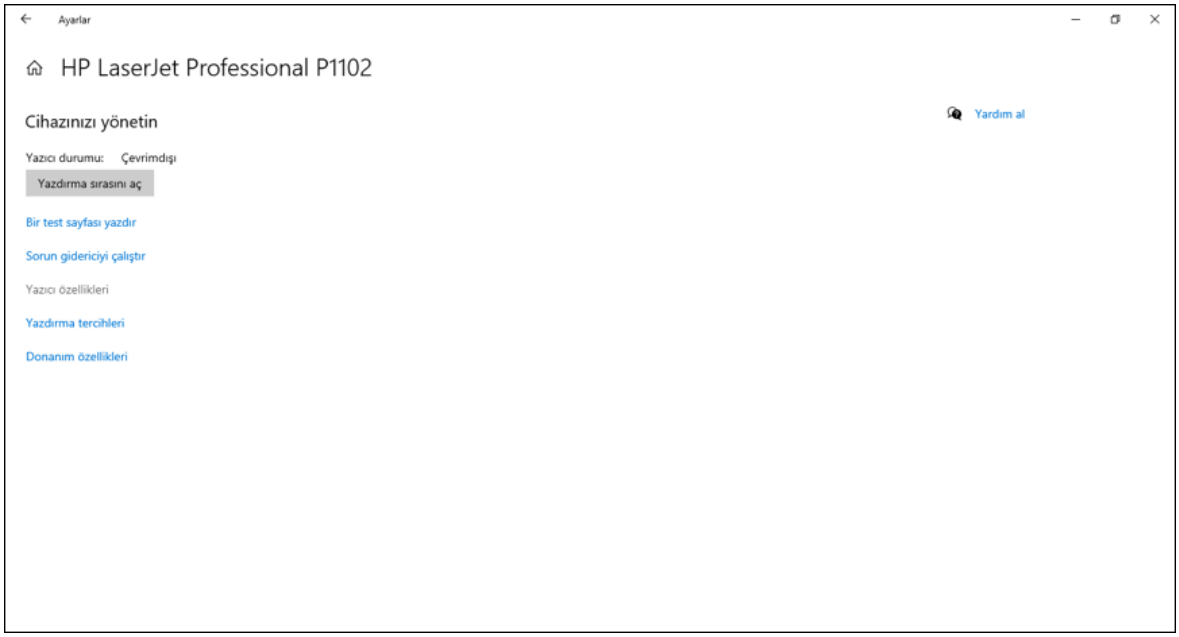
b) Ağ Üzerinde Kaynak Paylaşım Güvenliği

Ağ üzerinde kullanılan her bilgisayara yazıcı, tarayıcı gibi kaynakların alınması maliyet açısından problemler olabilir. Bu problemi çözmek adına kaynakların paylaşımı kullanılmaktadır. Kaynak paylaşımında da belli güvenlik risklerine dikkat edilmelidir. Burada sistemde tanımlı bir yazıcının Windows işletim sisteminde paylaşımı anlatılacaktır. Denetim masasından yazıcılar ve tarayıcılar ekranı Şekil 17'deki gibi açılır.



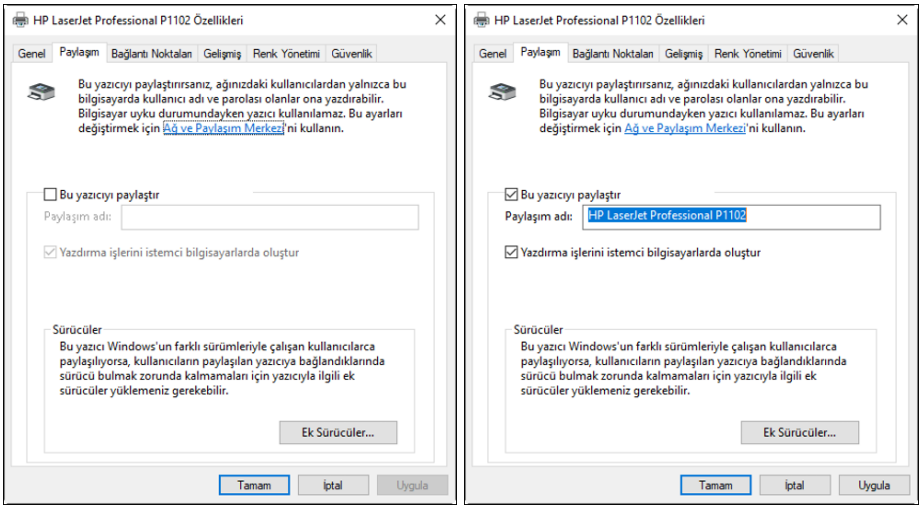
Şekil 17: Yazıcılar ve Tarayıcılar Penceresi

Yazıcı seçilerek gelen düğme seçeneklerinden “Yönet” seçilmelidir. Karşımıza Şekil 18’deki “Ayarlar” penceresi gelecektir. Bu pencere tanımlı yazıcının ayarlarını değiştirilmesini sağlayan bölümdür. Bu penceredeki “Yazıcı Özellikleri” bölümü seçilmelidir.



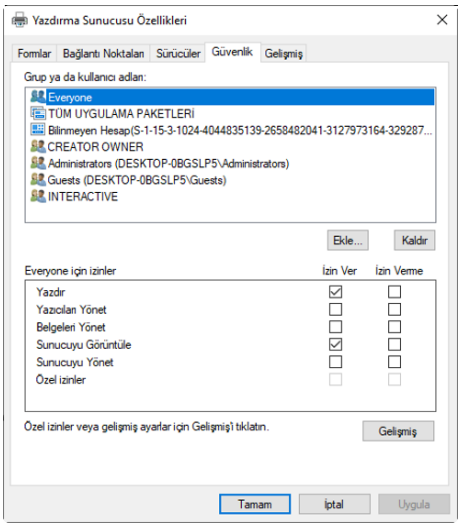
Şekil 18: Yazıcı Ayarlar Penceresi

Şekil 19’daki yazıcı özellikleri penceresi karşımıza gelir. Yazıcı özellikleri penceresinde ise “Paylaşım” sekmesi seçilmelidir. Bu pencere paylaşımın açılacağı bölümdür. “Bu yazıcıyı paylaş” onay kutusu seçildiğinde ağ üzerinde paylaşım adı aktif olur. Dilenirse ağ üzerinde görülecek isim değiştirilebilir. Aynı isimde farklı yazıcılar ağ üzerinde olabilir. Bunun için anlamlı isimler verilmesi ağ üzerinde bulunması adına kolaylıklar sağlayacaktır.



Şekil 19: Yazıcı Özellikleri Penceresi Paylaşım Sekmesi

Ağ üzerinde paylaşılan yazıcıya tüm kullanıcılar erişebilir. Bununla ilgili belirli kısıtlamalar getirmek güvenlik açısından bazı riskleri ortadan kaldıracaktır. Yazıcı özellikleri penceresinde "Güvenlik" sekmesi seçilmelidir. Şekil 20 karşımıza gelecektir. Burada hangi kullanıcılara yetki verilecekse seçilerek gerekli izinler verilebilir ya da verilen izinler kaldırılabilir.



Şekil 20: Yazıcı Özellikleri Penceresi Güvenlik Sekmesi

ÖZET

İşletim sistemi kullanıcıya bilgisayar kaynaklarını verimli bir şekilde kullanabilmesini sağlayan yazılım bütünüdür. Çoğu sistem küçük parçaların bir araya gelmesiyle oluşmuştur. Dosyalar İşletim sisteminin yapısı içerisinde hücreler gibidir, dosyalar ise bir anlamlı bir bütün olarak birleştiğinde ise klasör kavramına tekabül etmektedir. Dosya ve klasör yapıları yazılım bölümlerinin temel yapıtaşlarıdır. Klasörler aynı yapıya ait olan dosya ve klasörlerin anlamlı bir bütün oluşturmasını sağlayan yapılardır. Dosya, disk üzerinde depolanmış verilerin bütününe verilen isimdir. Dosya, birbiriyle ilişkili veriler topluluğunu bir saklama ünitesinde saklamak amacıyla kullanılan yapıdır.

Dosya sistemi, bir dosyanın bir disk üzerinde nasıl saklandığı ve bir bilgisayarın dosyaları yönetebilmek için erişimi nasıl sağladığını kontrol eden bir sistemdir. Farklı işletim sistemleri olduğundan her bir sistemin dosya sistemi farklıdır. NTFS, HPFS, DOS, FAT 16/32, HFS, ISO 9660 ve Ext gibi dosya sistemleri kullanılmaktadır.

Windows ve Linux işletim sistemlerinde farklı dosya sistemleri kullanılmaktadır. Windows ticari, Linux açık kaynaklı bir yazılımdır. Çekirdek yapıları farklıdır. Linux daha güvenli bir çekirdek yapısına sahiptir. Linux düşük özellikli bilgisayarlarda iyi bir performans göstermektedir. Linux kök dizin ağaç yapısındadır, Windows'ta ise sürücülerin altında klasör yapısı bulunur. Linux'ta sistem ve program dosyalarını farklı dizinlerde bulabilirsiniz, oysa Windows'ta sistem ve program dosyaları genellikle C: sürücüsüne kaydedilir.

Erişim kontrol listeleri (Access Control List – ACL), kullanıcıları ve grupları belirli erişim yetenekleriyle ilişkilendirir. Dosya ve klasörlerin güvenliği için izinler çok önemlidir. Sistemin sürdürülebilirliği açısından öznitelikler ayarlanmalıdır. Güvenlik ilkesi oluşturarak dosya ve klasör güvenlik politikası oluşturmak mümkündür. Paylaşılan Kaynakların kullanım yetkileri ayarlanırken dikkat edilmesi gereken izinler örneklendirilmiştir.

SORULAR

1. İşletim sistemlerinde neden farklı dosya sistemleri bulunmaktadır?
2. Kaynak paylaşımının güvenli bir şekilde olabilmesi için neler yapılmalıdır?
3. Erişim kontrol listelerinin İşletim Sistemleri açısından önemi nedir?
4. Dosya güvenliğinde hangi özelliklere dikkat edilmelidir?
5. Windows ve Linux karşılaştırıldığında hangi işletim sistemi güvenlik anlamında daha başarılıdır, sebebiyle birlikte açıklayınız?
6. Klasör güvenliğini sağlamak için neler yapılmalıdır?
7. Farklı işletim sistemlerindeki izinler neden bütün kullanıcılara tam yetkili olarak tanımlanmamalıdır?
8. Ağ üzerinde dosya ve klasör paylaşımında “Everyone” kullanıcısına tam yetki vermenin sakıncaları nelerdir?
9. İşletim sistemlerinde dosya kavramı neden önemlidir?

KAYNAKLAR

Apple. (t.y.). *Mac'te dosya, klasör veya diskler için izinleri değiştirme*. Erişim Tarihi: 03 16, 2021, macOS Kullanma Kılavuzu URL: https://support.apple.com/tr-tr/guide/mac-help/mchlp1203/mac

Aydınalp, A. (2013). *İşletmenlik Ders Notları*. Özel Berkcan Bilgisayar Kursu.

Başaranoğlu, E. (2015, 07 26). *Windows Ortamında Erişim Kontrol Listeleri*. Erişim Tarihi: 03 12, 2021, Siberportal URL: https://www.siberportal.org/blue-team/securing-operating-systems/securing-windows-operating-system/access-control-list-on-windows/

Boyan, F. (2020, 05 31). *Windows Server 2019'da Dosya ve Klasör Paylaşım İzinleri Bölüm-1*. Erişim Tarihi: 03 16, 2021, fıratboyan URL: https://www.firatboyan.com/windows-server-2019-ntfs-sharing-paylasim-izinleri-dosya-klasor-yetkilendirme-bolum-1.aspx

Bradley, T. (2020, 09 11). *Configuring Unix/Linux File and Directory Access Rights*. Erişim Tarihi: 03 14, 2021, lifewire URL: https://www.lifewire.com/configuring-unix-linux-file-2487531

Coşar, M. (2015). İşletim Sistemi Ders Notları. Çorum: Mühendislik Fakültesi/Bilgisayar Mühendisliği Bölümü.

Kurt, B. (2005). İşletim Sistemleri. İstanbul: İstanbul Teknik Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü.

Mesut, Y. (2016). *İşletim Sistemleri Ders Notları*.

nongraper. (2019, 03 14). *Windows 10: Ağ Konumu (Ağ Paylaşımı) Ayarları*. Erişim Tarihi: 03 14, 2021, Site Adı: nongprader.net URL: https://nongprader.net/windows-10-ag-konumu-ag-paylasimi-ayarlari/

Samet, D. (2018). Dosya Sistemleri. *Bilgisayar Sistemleri (Bölüm 1 Ek Sunum)*. Ankara: Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü.

Taşcı, T. (2013). 2. Hafta - İşletim Sistemleri . *Temel Bilgi Teknolojisi Kullanımı*. Sakarya Üniversitesi Bilgisayar ve Bilişim Bİliimleri Fakültesi.

Türkoğlu, İ. (2006). BİL391 İşletim Sistemleri (Ders Notları). Elazığ: Fırat Üniversitesi TEF Elektronik ve Bilgisayar Bölümü.

Yalçın, N. (2015). İşletim Sistemleri Ders Notları. Ankara: Gazi Üniversitesi Bilgisayar ve Öğretim Teknolojisi Eğitimi Bölümü.