ISTANBUL UNIVERSITY ENGINEERING FACULTY **YEAR : 2002 (405-408)**
JOURNAL OF ELECTRICAL & ELECTRONICS VOLUME : 2
NUMBER : 1

BÝLGÝSAYAR SÝSTEMLERÝNDE ERÝÞÝM KONTROLU

ACCESS CONTROL IN COMPUTER SYSTEMS

Tayfun KAYNA[a] [1] Fikret HÜR[2] Serhat [a] EKER[3]

[1]Ýstanbul Üniversitesi, S.B.M.Y.O [2]Güven Bilgisayar Ltd.[a] ti.
[3] Ýstanbul Teknik Üniversitesi, Elektrik Mühendisliði Bölümü

ÖZET

Bu çalýþmada, genel anlamda eriþim kontrol teknikleri ve özel olarak da Güvenliklik Amaçlý Eriþim Kontrol Sistemlerinden söz edilmiþtir. Ayrýca 32-bit windows, exe dosyalarýnýn kontrol altýna alýnmasýna iliþkin bir örnek verilerek, konunun uygulamadaki çeþitliliði vurgulanmýþtýr.

Anahtar Kelimeler: *Eriþim kontrolu, 32 bit Exe Dosyasý, Otomatik Eriþim Kontrolu*

ABSTRACT

In this study, two aspects of access control in computer systems are presented. These are general purposed access control and Security Purposed Accesse Control techniques respectively. Also, an example was given to emphasize the importance of the security purposed access control for 32-bit EXE files that run under windows.

Key Words: *Access Control, 32- bit Exe file, Automatic Access Control*

1. GÝRÝÞ

Eriºim Kontrolu, bir nesneye (bina,bilgisayar sistemi,yazýlým,vb) sadece izni ve yetkisi olan kiþilerin ulaþabilmesini saðlayan sistemin genel adý olarak tanýmlanabilir. Bu geniþ konunun bir parçasý olan, "Bilgisayar Sisteminde Gizlilik Amaçlý Eriþim Kontrolu", bir bilgisayardaki yazýlýmlarýn, eriþim kontrol teknikleri uygulamasý ile izni olmayan kiþilerce kullanýlmasýný engellemek amacý taþýr. Ýþletim sisteminin eriþim kontrolünü kýsýtlayan seçenekleri olmasýna karþýlýk, bunlar çoðu zaman yeterli deðildir.

Bir yazýlým üzerine eriþim kontrol tekniði uygulandýðýnda baþka bir deyiþle koruma yapýldýðýnda o yazýlýmdan beklenenler aþaðýdaki gibi verilebilir.

- Yazýlým kopyalansa bile, izin verilmeyen baþka bir ortama taþýndýðýnda yazýlým çalýþmamalýdýr.
- Yazýlýmýn izinsiz olarak bir örneði çýkarýlsa bile , yazýlým çalýþýrken kontrol ettiði kontrol ortamýnýn (anahtar disket,hard disk, bilgisayarýn rom bilgileri, vb) benzer bir örneði çýkartýlmamalýdýr. Dolayýsýyla sistem, izin verilenin dýþýnda kullanýlmamalýdýr.
- Dosya üzerinde bulunan eriºim kontrol modülü ve dosyanýn içeriðinde bir deðiþikliðe izin verilmemelidir. Eðer bu

deðiþiklik uygulansa bile dosya normal fonksiyonuyla çalýþmamalýdýr.
- Eriþimi kontrol altýna alýnmýþ bir dosyanýn içeriði görülmemelidir.

Burada özellikle son madde çok önemlidir. Çünkü dosyanýn yapýsý incelenirse dosya içerisindeki eriþim kontrol modülü devre dýþý býrakýlabilir. Bu beklentiler göz önünde tutularak deðiþik teknikler oluþturulmuþtur. Bütün bu yöntemlerin amacý ayný olsa da, eriºimde kontrol ünitesi olarak kullandýklarý nesnelerin farklý olmalarýndan dolayý bu teknikler genellikle ünitelerin adlarýyla anýlmaktadýr.

2. ERÝÞÝM KONTROL TEKNÝKLERÝ

Eriþim kontrolünde amaç, yazýlýmýn kontrol altýna alýnmasýdýr. Bu noktada belirlenen, bunun nasýl yapýlacaðýndan çok, ne kullanýlarak yapýlacaðýdýr. Eriþim kontrolünün temelini ise seçilen kontrol ünitesi oluþturur. Bazý farklý kontrol üniteleri ile oluºturulmuº teknikler aþaðýdaki gibi verilebilir.

1. Anahtar – Disket Tabanlý Eriþim Kontrol Sistemi;
2. Bilgisayar Donaným Tabanlý Eriþim Kontrol Sistemi;
3. Hard-Disk Tabanlý Eriþim Kontrol Sistemi;
4. Diðer Eriþim Kontrol Sistemleri;

Eriþim kontrol sistemleri bilginin sayýsal ortamlarda tutulmaya baþlanmasýyla vazgeçilmez bir sektör haline gelmiºtir. Eriºim kontrol sistemleri farklý konulara ayrýlsa da genelde amacý, yetkisi olmayan kiþilerin korunan bilgiye veya nesneye eriºmesini engellemektir. Günümüzde bu konuda yapýlmakta olan çalýþmalar þöyle özetlenebilir :

1. Að ortamlarýnda disk paylaþýmý amaçlý eriºim kontrol sistemleri:
Kontrol, network iþletim sistemini hazýrlayan kuruluþlar tarafýndan yapýlýr. Hangi kullanýcýnýn hangi gruplarýn üyesi olacaðý ve hangi haklara sahip olacaðý gibi yetkiler dahilinde sisteme giriþ yapmayý hedefler.

2. Özel bir donaným gerektiren fiziksel koruma amaçlý eriþim kontrol sistemleri:
Barkod tabanlý sistemler, fotoðraf ve görüntü tanýma tabanlý sistemler, parmak izi tanýma tabanlý sistemler,göz retinasý tanýma tabanlý sistemler bu gruba örnek gösterilebilir.

3. Özel bir donaným gerektiren bilgiyi kullaným amaçlý eriþim kontrol sistemleri:
Manyetik kart tabanlý sistemler; Touch Memory ve EEPROM kullanýlarak yapýlmýþ sistemler, mikro-iþlemci kullanýlarak yapýlmýþsistemler.

3. GÝZLÝLÝK AMAÇLI ERÝÞÝM KONTROLU

Buradaki amaç, yetkisiz kiºilerin sisteme giriºinin engellenmesidir. Bu ºekilde tasarlanan sistem altý temel nokta üzerine kurulmuþtur :

1)Sistemin en önemli parçasýný, özel olarak tasarlanan Eriþim Kontrol Cihazý oluþturmaktadýr. Bu cihaz,sistemin anahtarý olarak kullanýlýr. Bir eriþim kontrol sisteminde bulunmasý gereken, simülasyona karþý koyabilme özelliði bu cihazla saðlanmýþtýr. Ayrýca sisteme ait tüm deðiþken bilgiler bu cihaz üzerinde tutulmaktadýr.

2)Dos iþletim sisteminde bulunan çalýþtýrýlabilir dosyalarýn eriþimlerinin kontrol altýna alýnmasý saðlanmýþtýr.

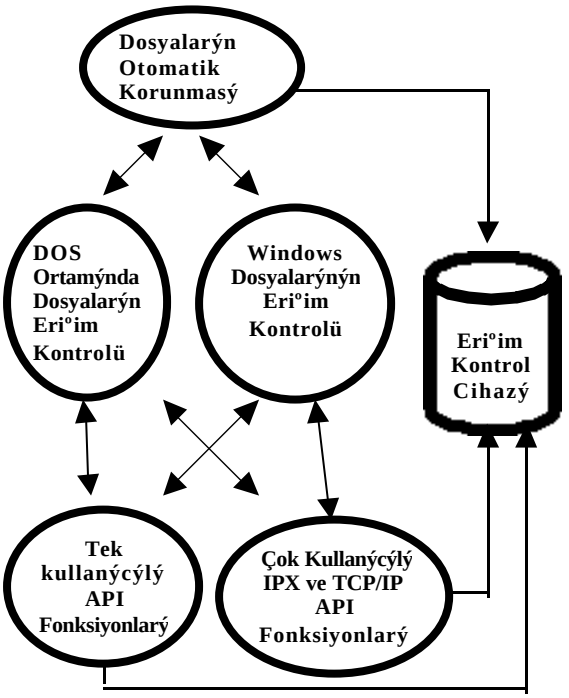
3)Windows 16 bit ve 32 bit EXE dosyalarýnýn eriþimlerinin kontrol altýna alýnmasý saðlanmýþtýr.

4)Tüm çalýþtýrýlabilir dosyalarýn (DOS, Windows 16 bit ve 32 bit EXE yapýsýnda), otomatik olarak korunabilmesi için gerekli olan yazýlýmlar hazýrlanmýþtýr.

5)Tek kullanýcýlý yazýlýmlar için yazýlým hazýrlanmasý sýrasýnda kullanýlmak üzere eriþim kontrol sisteminin fonksiyonlarýný içeren kütüphaneler (.lib,.obj,.dll) yaygýn seviyeli programlama dilleri için hazýrlanmýþtýr.

6)IPX ve TCP/IP protokollerini kullanan çok kullanýcýlý ortamlarda çalýþacak yazýlýmlarýn eriþimlerinin kontrol altýna alýnmasý saðlanmýþtýr. Bunun için öncelikle tek bir Eriºim Kontrol Cihazý'nýn kullanýlabilmesi için haberleþmeyi ve sistemin yönetimini yapan bir server yazýlýmý hazýrlanmýþtýr. Buna ek olarak yazýlýmýn hazýrlanmasý sýrasýnda kullanýlmak üzere eriþim kontrol sisteminin fonksiyonlarýný içeren kütüphaneler (.lib,.obj,.dll) yaygýn üst seviyeli programlama dilleri için hazýrlanmýþtýr.

Bu altý birimin iliþkileri Þekil 1. de görülmektedir.



Þekil 1. Eriþim kontrolu iletiþim diyagramý.

Section table'a Eriºim Kontrol Modülü'nü Ýçeren section (.pcode) eklenir

Eriºim Kontrol Modülü dosya sonuna eklenir.

Programýn baþlangýç noktasý Eriþim Kontrol Modülünün baþlangýcýný Gösterecek þekilde deðiþtirilir.

Orijinal Entry Point RVA ise bu Section üzerinde bir yerde saklanýr.

Orijinal programýn kod alanýný Eriþim kontrol cihazýndaki key deðeri olarak ºifrelenir.

Eklenmiþolan .pcode kod alanýna anti debugging,data alanýna ise þifreleme uygulanýr.

Disk üzerinde yapýlan bu iþlemler son aþama olarak dosya üzerine yazýlýr.

ªekil 2. 32-bit çalýþtýrýlabilir dosyalarýn eriþiminin kontrol altýna alýnmasý.

4. 32-BÝT WÝNDOWS –EXE DOSYALARININ ERÝÞÝMÝNÝN KONTROL ALTINA ALINMASI

32-Bit Windows EXE Dosyalarýnýn Eriþiminin Kontrol Altýna Alýnabilmesi için ilk olarak eriþim kontrol ile ilgili kod ve data alanlarýný bulunduran ve .pcode olarak adlandýrýlan section,dosyanýn sonuna eklenir.Daha sonra programýn baþlangýç noktasý (Entry Point RVA), eriºim kontrol kodunun baºlangýç noktasýný gösterecek þekilde deðiþtirilir. Orijinal Entry Point RVA, pcode section üzerinde saklanýr. Orijinal programýn kod alaný (çoðunlukla itext section), Eriþim kontrol cihazýndan alýnan yapay random deðerler, key deðeri olarak kullanýlarak ºifrelenir. Eklenmiþ olan pcode section'ýn kod alanýna anti-debugging data alanýna ise þifreleme uygulanýr. Bu aþamaya kadar disk üzerinde yapýlan bu iþlemler dosya üzerine yazýlýr.

Yapýlmasý gereken iþlemlerin akýþ diyagramý þeklindeki görüntüsü aþaðýdaki gibidir:

5. SONUÇLAR VE ÖNERÝLER

Bu çalýþmada bilgisayar sisteminde eriþim kontrolu ve özel olarak da gizlilik amaçlý eriþim kontrolu hakkýnda bilgi verilmiþtir.Ayrýca konunun bir uygulamasý olarak da 32 bit Windows EXE dosyalarýnýn eriþim kontrolunun nasýl yapýlacaðý bir algoritma ile gösterilmiþtir.Yapýlan bu çalýþma sözkonusu gizlilik eriþim kontrol sistemlerinde güvenliði de önemini ön plana çýkartmaktadýr.Bu baðlamda güvenliðin artýrýlmasý için bir cihaz ve algoritma da geliºtirilebilir ve eriºim kontrol sisteminde olmasý gereken simülasyona karþý koyabilme özelliði, yine bu cihaz ve algoritmalarýn birlikte kullanýlmasýyla saðlanabilir.

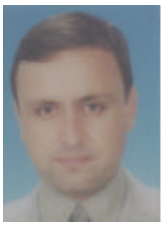
KAYNAKLAR

[1] Bowers Don M, "Access Control and Personal Identification Systems," 2.Baský, Butterworth-Heinemann, 1999.

[2] Konicek J.,Little K.,Security, Id Systems and Locks : "The Book on Electronic Access Control," 2.Baský, Butterworth-Heinemann, August 1997.

[3] Pietrek M., "Windows 95 System Programming Secrets," 2.BASKI; IDG Books Worldwide Inc., 1995.

[4] Hür F., "Bir Bilgisayar Sisteminde Gizlilik Amaçlý Eriþim Kontrolü," Doktora Tezi , Ý.Ü. Bilgisayar Mühendisliði Bölümü, Mayýs 1999.



Tayfun KAYNAª ; 1964 yýlýnda Ýstanbul'da doðdu.Ý.Ü.Ýþletme fakültesinden lisans(1986),ayný üniversiteye baðlý Sosyal Bilimler Enstitüsü Kantitatif Analizler ve Programlama bölümünden yüksek lisans (1990) ve Ý.Ü.Fen Bilimleri Enstitüsü Bilgisayar Mühendisliði programýndan doktora (1997) ünvanýný aldý. Özel sektörde çeþitli firmalarda programcý olarak çalýþtý. Halen Ý.Ü.S.B.M.Y.O. bünyesindeki bilgisayar derslerini vermek üzere öðretim görevlisi olarak çalýþmaktadýr.

Fikret Hür, 04.04.1966 tarihinde Zonguldak'ta doðdu. Ýlk, orta ve lise eðitimini Zonguldak'ta tamamladý.
Yýldýz Üniversitesi Bilgisayar Bilimleri Mühendisliði Bölümünde, 1983 yýlýnda baþladýðý lisans eðitimini 1987 yýlýnda tamamladý. Lisans bitirme tezinde, "**CMOS tümdevrelerin ve EPROM'larýn statik testleri**", konusunda, bir çalýþma yaptý. 1988 yýlýnda, Enka A.Þ.'nin bilgi iþlem merkezinde yazýlým geliþtirme mühendisi olarak 1 yýl süreyle çalýþtý.
1988 yýlýnda, Mimar Sinan Üniversitesi Fen Bilimleri Enstitüsü Endüstri Ürünleri Tasarýmý Ana Bilim Dalýnda, baþladýðý yüksek lisans programýný, 1991 yýlýnda tamamladý. Yüksek lisans tezinde, "**Dörtlü Ocak Kontrol/Gösterge Ýliþkisinin Düzenlenmesinde, Düzlemsel Ýliþki ve Uzaysal Uygunluða Ait Genel Ýlkeler**" konusunda bir çalýþma yaptý.
Ý.Ü. Bilgisayar Bilimleri Mühendisliði Bölümünde, 1991 yýlýnda baþladýðý doktora programýný, 1999 yýlýnda sunduðu "**Bir bilgisayar sisteminde gizlilik amaçlý eriþim kontrolü**" adlý doktora tezi ile tamamladý.
Çeþitli projelerde programcý-sistem analist ve yönetici olarak çalýþtý. Son olarak da TUBÝTAK tarafýndan desteklenen, "**Veri Toplama Terminali Geliºtirmesi**" adlý projenin yöneticiliðini yaptý.

Serhat ª eker; 1959 Ýstanbul'da doðdu. Ý.T.Ü.Elektrik Elektronik Fakültesini bitirdi.Ayný üniversitede yüksek lisans çalýþmalarýný tamamladý.Daha sonraki yýllarda doktor ve doçent ünvanlarýný aldý. Araþtýrmalarýný Neural Network konusunda yoðunlaþtýrdý. Halen Ý.T.Ü.Elektrik Elektronik Fakülteside öðretim üyeliðine devam etmektedir