Güvenlik Amaçlı Dosya Takip Programı

İsmail KURNAZ[1], Doğan ÇALIKOĞLU[2]

Elektronik Bilgisayar Eğitimi Bölümü, Karabük Üniversitesi, Karabük, Türkiye[1]
Bilgisayar Eğitimi Bölümü, Gazi Üniversitesi, Ankara, Türkiye[2]
ikurnaz@karabuk.edu.tr[1], dcalik@gazi.edu.tr[2]

Özet— Bu çalışmada, Windows işletim sistemleri altında çalışan uygulamaların listesini kullanıcıya gösteren DOST isimli bir dosya takip programı geliştirilmiştir. Sistemde çalıştırılan uygulamaların listesi bazı özel kütüphane fonksiyonları kullanılarak oluşturulmuştur. DOST, 16 bit ve 32 bit NT sistemlerde PSAPI kütüphane fonksiyonları, 9x/2000/Me/XP/Vista sistemlerde Tool Help kütüphane fonksiyonları kullanılarak çalışan uygulamalara ait süreçlerin, modüllerin ve ipliklerin listelenmesini gerçekleştirir. Uygulamalar listelenirken kullanılacak kütüphane fonksiyonları DOST'un çalıştığı işletim sistemini algılama yeteneği sayesinde belirlenir. Kullanıcılar bilgisayarları ile çalışırken, sistemde çalışan bütün uygulamaların listesini DOST'un her zaman üst pencere olarak kalabilme yeteneği sayesinde takip edebilirler.

Anahtar kelimeler— Bilgisayar Güvenliği, Toolhelp fonksiyonları, PSAPI fonksiyonları, Süreçlerin listelenmesi, Modüllerin listelenmesi, İpliklerin listelenmesi

Program of File Monitor for Security

Abstract— In this study, a file monitor program whose name is called as DOST has been developed. DOST can show the list of the running applications in the Windows operating systems to the users. The list of currently running applications has been implemented by using some of the special library functions. DOST implements to enumerate running applications and their processes, modules and threads by using PSAPI library functions in NT systems and by using Tool Help library functions in 9x/2000/Me/XP/Vista systems. Which library's function will be used while the applications are enumerated, determine by the ability of DOST's perceiving operating system. While the users study with their computers, they can monitor the list of all currently running applications by the ability of DOST's always on top window property.

Keywords— Computer Security, Tool Help functions, PSAPI functions, Enumerating processes, Enumerating modules, Enumerating threads.

1. GİRİŞ

Bilgisayar kullanırken, kullanıcının bilerek çalıştırmadığı fakat sistemde çalışan birçok program vardır. Kullanıcı bu programların çalıştığını sabit diskin veya ağ kartının ışığının yanıp sönmesinden anlamaktadır. Yürütülen bu faaliyetlerin istenen veya istenmeyen bir faaliyet olduğunu belirlemek önem taşımaktadır. Kullanıcı bilgisayarın kendi hâkimiyetinde işlem görmesini beklerken, bu tip işlemler "kullanıcısına rağmen" yürütülüyor olabilir. Yapılan işlemlerde bilgisayar sahibinin verileri bir yerlere gönderiliyor ve yahut bilgisayar sahibine ait bazı özel bilgiler (şifreler gibi) başkaları tarafından öğreniliyor olabilir. DOST bu gibi durumları ortaya çıkarmak amacı ile geliştirilmiştir.

DOST'un hazırlanmasının nedenleri şunlardır:

1. Bilgisayarın kontrolünün kullanıcıdan çıkmasını önlemek,
2. Bilgisayara karşı dış tehditleri engellemek,
3. Casus yazılımları engellemek,
4. Windows işletim sisteminde perde arkasında gerçekleştirilen işlemleri öğrenmek.

Sistemde gerçekleştirilen olayları takip etmek için kullanılan bir çok çeşit program vardır. Bu programlar gerçekleştirdikleri faaliyetlere göre dosya takip programları, kayıt düzenleyicisini izleyici programlar, ağ paketlerini izleyici programlar, sabit disk izleyici programlar, port takip programları ve hata ayıklayıcılarını izleyici programlar olarak sınıflandırılabilir.

2. DOSYA TAKİP PROGRAMLARI

DOS, Windows 3.xx gibi eski nesil işletim sistemleri ve yeni nesil Windows işletim sistemleri

(9x/Me/NT/2000/XP) her bir sürece adres alanı ayırmak için karmaşık mekanizmalara sahiptirler. Bu mimari gerçek bir bellek koruması sağlar. Böylece hiçbir uygulama başka bir sürecin adres alanını bozamaz ve işletim sisteminin kendisine zarar vermesini engeller. Bu gerçek sistemi gözetleyen uygulamalar geliştirilmesini de zorlaştırır. [1]

Çalışan uygulamaları veya bu uygulamaların süreçlerini (process), ipliklerini (thread), pencerelerini, modüllerini vb. görüntülemek için aşağıdaki yöntemler kullanılır:

1. ToolHelp32 veya PSAPI (Process Status Application Programming Interface) kütüphane fonksiyonları. [2]
2. Windows ileti sistemi ve kanca fonksiyonları (hook functions). Windows işletim sisteminde bir uygulamanın çalıştırılabilmesi için iletiler kullanılır. İletiler ile uygulamalar arasına kanca fonksiyonları yerleştirilerek sistemde işlenen tüm iletiler kontrol edilebilir. Kanca fonksiyonlarından dönen veya elde edilen değerler ile sistemde çalıştırılan bütün dosyalar sıralanabilir. Filemon programı kanca fonksiyonları kullanılarak hazırlanmış bir dosya takip programıdır. [3]

Windows işletim sisteminde cereyan eden olayların listesini oluşturabilmek için Windows işletim sisteminin sürümüne göre iki ayrı özel kütüphane fonksiyonları kullanılır: Windows 9x/2000/Me/XP sistemlerde Tool Help kütüphane fonksiyonları, NT sistemlerde PSAPI kütüphane fonksiyonları.

Tool Help fonksiyonları, program geliştiricilere çalıştırılan Microsoft Win32 tabanlı uygulamalar hakkında daha kolay bilgi vermek için kullanılırlar. Bu fonksiyonlar Windows tabanlı hata ayıklama uygulamalarını temel alarak tasarlanmışlardır.[4]

Windows NT sistemlerinde cereyan eden olayların listesini oluşturmak için PSAPI fonksiyonları kullanılırlar. PSAPI fonksiyonları kullanılarak sistemde çalıştırılan bütün uygulamaların ve bu uygulamalara ait süreçlerin ve modüllerin listesi oluşturulabilir. Çalışan iplikleri listeleyecek PSAPI fonksiyonu yoktur. Windows 2000/XP gibi NT tabanlı işletim sistemlerinde ipliklerin listesini oluşturmak için Tool Help kütüphane fonksiyonları kullanılabilir.[5]

Windows işletim sistemi bir GUI (Graphical User Interface) uygulamasıdır. GUI uygulamalarında ileti tabanlı bir çalışma biçimi söz konusudur. Klavye, fare vb. girdi birimlerinden alınan bilgilere ileti denir. Bir girdi işlemi oluştuğunda bunu önce sistem, kendisi alır ve sonra bu girdi işlemi hangi programa ilişkinse o programa gönderir. Bu yüzden Windows da ki programlama modeli gelen iletinin yorumlanarak işlenmesi temeline dayanır[6].

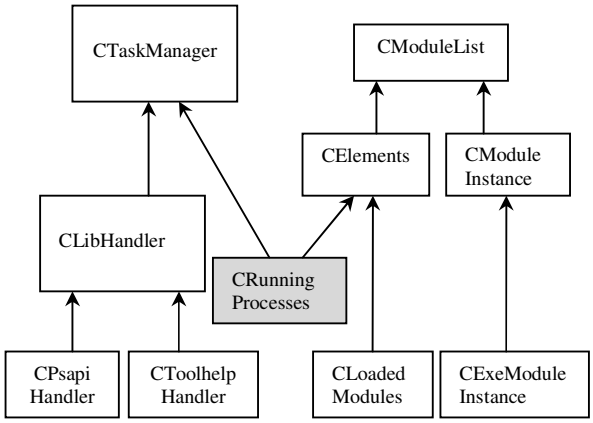
İletiler diğer işletim sistemlerinde olduğu gibi Windows işletim sisteminin de önemli parçalarıdırlar. Bir Windows programında GetMessage()/DisPatchMessage() gibi fonksiyonlar programın işlevlerini yürüten parçaları, pencere yordamları ve bunlara ilişkin fonksiyonlar gibi iletilerde programın etkileşim noktalarını ifade ederler. Bir Windows programında iletilerin işlenmesi durdurulursa programın çalışması da durdurulur. Sadece program sonlanmakla kalmaz, bu sirkülasyon devam etmezse diğer programlar da durur. [7]

Windows da iletiler pek çok amaç için kullanılmaktadırlar. Fare hareketleri veya fare tuşlarına tıklanması, klavye tuşlarına basılması, menü seçimleri gibi olaylar iletiler ile gerçekleştirilir. İletiler sistemde gerçekleştirilen olayları araştırmak için de kullanılır. Örneğin iletiler Windows'un kapatılabilmesi için diğer bütün programların uygun olup olmadığını anlamak için kullanılırlar.[8]

3. DOST DOSYA TAKİP PROGRAMI

DOST, sistemde cereyan eden olayları takip etmek için Windows İleti Sistemini kullanarak sistem çalışırken hali hazırdaki bütün olayların kopyası alır. Bu olayların gerçekleşmesi için çalışması gerekli bütün dosyalar NT sistemlerde PSAPI fonksiyonları, diğer Windows sistemlerinde ise Tool Help fonksiyonları ile görüntülenir. Kullanıcılar bilgisayarları ile çalışırken, sistemde çalışan bütün uygulamaların listesini DOST'un her zaman üst pencere olarak kalabilme yeteneği sayesinde takip edebilirler.

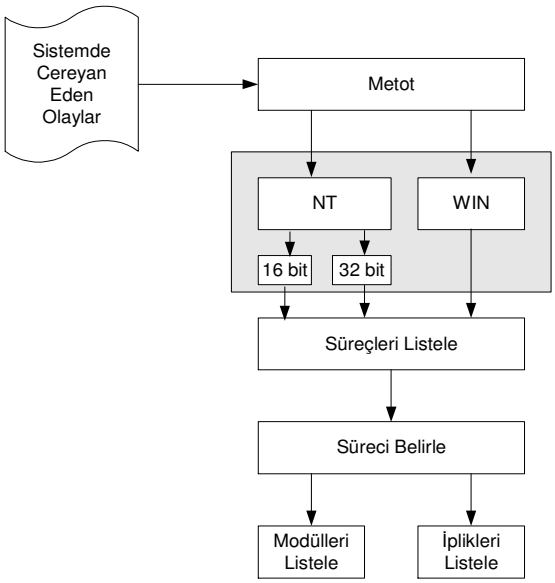
DOST programı birçok yordamdan oluşmuştur. Bu yordamlar hali hazırda yürütülen süreçleri tespit etmek, listelemek, süreçlere ait modülleri ve iplikleri meydana çıkarmak ve bu modül ve iplikleri listelemek için kullanılmışlardır.



Şekil 1. Süreçlerin Sıralandırılması

Şekil 1'de sistemde çalışan süreçlerin sıralanmasını sağlayan alt sistemler ve bunların birbirleri arasındaki ilişkiler gösterilmiştir. Burada yer alan CTaskManager öğesi sistemin işlemcisi yerindedir. CTaskManager, kullanılan işletim sistemine göre tercih edilmesi gereken fonksiyon kütüphaneleri için bir yürütücü değer üretmekle sorumludur (CLibHandler). Süreçler hakkında doğru bilgi elde edebilmek için doğru kütüphane ile çalışmak gereklidir. CTaskManager, CPsapiHandler (veya

CToolhelpHandler) parametre değerlerine göre hali hazırdaki aktif süreçlerin bir listesini hazırlar ve bu listeyi bekletir. Oluşturulan listedeki bütün süreçlerin sıralanması, DLL (dynamic link library) kütüphane dosyalarına erişilmesi, tutuldukları hiyerarşi bilgileri gibi verilere başka fonksiyonlar çağrılarak erişilebilir.



Şekil 2. DOST'un Temel Blok Şeması

Şekil 2'de yapılan çalışmanın blok şeması gösterilmiştir. Sistemde cereyan eden olayları tespit etmek için öncelikle hangi metodun kullanılacağı belirlenir. Windows 9x/Me işletim sistemlerindeki tüm uygulamalar WIN metodu ile tespit edilir. Windows 2000/XP işletim sistemlerinde 32 bit uygulamalar WIN metodu ile tespit edilirler. Windows NT/2000/XP işletim sistemlerindeki 16 bit uygulamalar NT-16 bit metodu ile tespit edilebilir. Windows NT işletim sistemlerinde 32 bit uygulamalar NT-32 bit metodu ile tespit edilirler. 16 bit ve 32 bit uygulamalar için farklı yöntemlerin kullanılmasının sebebi NT/2000/XP işletim sistemlerinde DOS işlemlerinin bir sanal DOS sürücüsü ile gerçekleştirilmesinden kaynaklanmaktadır.[9]

Kullanılan işletim sistemi belirlendikten sonra ilgili fonksiyonlar kullanılarak çalışan süreçlerin listesine erişilir. İlk olarak listedeki ilk süreç getirilir. Bu sürecin listedeki son süreç olma durumu kontrol edilir. Son süreç ise ilk süreç, süreç listesine eklenir ve süreç listesi görüntülenir. Son süreç değilse listedeki sonraki süreç çağrılarak süreç listesine eklenir. Bu işlemler listedeki süreçler bitene kadar sürdürülür. Son süreç de süreç listesine eklendikten sonra sistemde çalışan süreçler görüntülenir.

Süreç listesinde yer alan herhangi bir sürecin modüllerini veya ipliklerini listelemek için ilgili süreç seçilmelidir. Bir sürece ait modüller şöyle listelenir:

İlk olarak seçili sürecin ilk modülüne erişilerek, ilk modül, modül listesine eklenir. Erişilen modülün son modül olma durumu kontrol edilir. Son modül ise modül listesi görüntülenir. Son modül değilse, modüller bitene kadar sonraki modüller çağrılarak modül listesine eklenirler. Eklenecek modül kalmadığında modül listesi görüntülenir.

Bir sürece ait iplikleri listelemek için seçili sürecin ilk ipliğine erişilerek, ilk iplik, iplik listesine eklenir. Erişilen ipliğin son iplik olma durumu kontrol edilir. Son iplik ise iplik listesi görüntülenir. Son iplik değilse, iplikler bitene kadar sonraki iplikler çağrılarak iplik listesine eklenirler. Eklenecek iplik kalmadığında iplik listesi görüntülenir.

4. GELİŞTİRİLEN YAZILIM

Bu çalışma Microsoft Visual C++ nesne yönelimli programlama dili kullanılarak hazırlanmıştır.

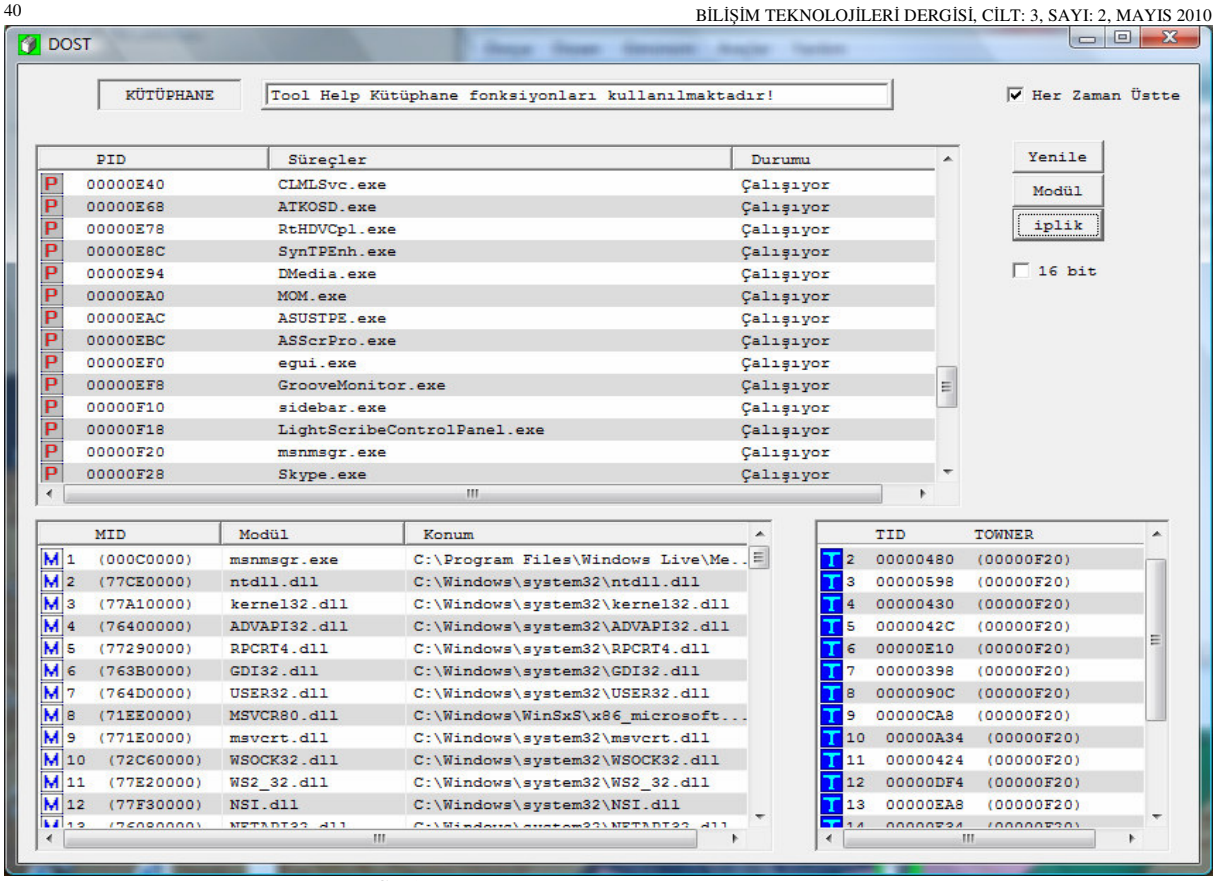
Şekil 3'de DOST programının kullanıcı ara yüzü yer almaktadır. Sistemde çalıştırılan süreçler ve ilgili sürece ait modüller ve iplikler üç ayrı liste kutusunda listelenmektedir. DOST, 100 ms (mili saniye) periyotlarla sistemde çalıştırılan süreçlerin listesini tazeler. Kullanıcı hangi sürece ait modülleri ve iplikleri görüntülemek istiyorsa süreç listesinden ilgili süreci belirler ve modül veya iplik düğmesini işaretleyerek çalıştırılan sürecin modüllerini ve ipliklerini ilgili liste kutusunda görüntülenmesini sağlayabilir. Şekil 3'de "msnmsgr.exe" sürecine ait modüller ve iplikler görüntülenmiştir.

5. SONUÇLAR

Bu çalışmanın tamamlanması ile bilgisayar kullanılırken işletilen programların ve bu programlara ait süreçlerin, modüllerin, ipliklerin listelenmesi başarılmıştır. Kullanıcı geliştirilen bu program ile sistemde cereyan eden bütün olayların listesini takip edebilecek bir araca sahip olmuştur.

Bilgisayar ile yapılan işlemlerin nasıl gerçekleştirildiği konusu giderek bir bilinmeyen haline gelmektedir. Yapılan bu çalışma ile bu bilinmeyen olayların önüne geçilerek, gerçekte nelerin olduğu ve nasıl gerçekleştirildiği sorularına cevaplar bulmaya yardım edecek bir araç geliştirilmiştir.

Sistemde çalışan uygulamaları ve bunların alt yordamlarını listelemek için özel kütüphane fonksiyonları kullanılmıştır. Özel kütüphane fonksiyonları (Tool Help veya PSAPI) kullanılarak sistemde çalışan uygulamaların ve bu uygulamaların alt yordamlarının izlenmesi, kanca fonksiyonlarına nazaran daha kolay gerçekleştirilebilir. Dosya takibi için sadece gerekli Tool Help (veya PSAPI) fonksiyonları ve bunların eriştiği yapıları bilmek yeterlidir.



Şekil 3. DOST programının kullanıcı ara yüzü

Kütüphane fonksiyonları çalışan uygulamaları, sistemin o andaki durumunun görüntüsünü alarak listelerler. Yani sistemi sadece bir anlık meşgul eder. Bu yüzden sistem performansına olumsuz etkileri yok denecek kadar azdır. Kütüphane fonksiyonları ile sistem fonksiyonları özdeş yapıda olduklarından dolayı kütüphane fonksiyonları çalıştırılırken sistem hasarlarına, çökmelere, uyuşmazlıklara neden olmazlar.

Hazırlanan bu uygulama ile sistemde gerçekleştirilen bütün olaylar takip edilebilir. Sistemde çalıştırılan fakat Ctrl+Alt+Del tuşlarına basıldığında çalıştığı gösterilmeyen uygulamalar da bu çalışma ile görüntülenebilmiştir. Bu sayede çalışan uygulamalar arasında casus yazılımlar gibi istenmeyen programlar tespit edilerek, sistemden kaldırılması sağlanabilir. Sistem bir uygulamayı çalıştırırken yaptıkları takip edilerek işletim sistemlerinin çalışma prensipleri kavranabilir.

Bu çalışma ile sistemde cereyan eden bütün olayların listelenmesi başarılmıştır. Çalışmanın bir sonraki adımında iyi niyetli yazılımlar ile kötü niyetli yazılımlar etiketlendirilebilir. Bu işlem şöyle gerçekleştirilebilir:

Bilinen kötü niyetli veya iyi niyetli yazılımlara eklenti olarak gelen kötü niyetli yazılımlar bir veri tabanında tutulurlar. DOST'un listesini tuttuğu dosya isimleri ile bu veri tabanında bulunan dosya isimleri karşılaştırılarak kötü niyetli olanlar bir işaretle belirtilir. Böylece kullanıcı çalışan uygulamaların hangisinin kötü niyetli olduğunu görebilir. Kötü niyetli uygulamaların sistemden kaldırılmasına da imkân tanınabilir.

KAYNAKLAR

[1] J. M. Hart, **Win32 System Programming 2nd Ed.,** Addison Wesley, Boston, A.B.D., 2000.
[2] Internet: P. Matt, Under the Hood, http://www.microsoft.com/msj/archive/S2058.aspx, 10.04.2010.
[3] Internet: M. Russinovich, B. Cogswell, Examining VxD Service Hooking: Monitoring, altering, or otherwise changing parts of Windows, http://www.ddj.com/184409878, 10.04.2010.
[4] W. A. Redmond, **Programmer's Guide to Microsoft Windows 95**, Microsoft Press, A.B.D., 1995.
[5] B. E. Rector, J. N. Newconer, **Win32 Programming**, Addison Wesley, Boston, A.B.D., 1997.
[6] M. Pietrek, **Windows Internals**, Addison Wesley, Boston, A.B.D., 1994.
[7] C. Petzold, **Programming Windows 5th Ed.**, Microsoft Press, A.B.D., 1998.
[8] P. Dabak, S. Phadke, M. Borate, **Undocumented Windows NT,** M&T Books, A.B.D., 1999.
[9] S. Schreiber, **Undocumented Windows 2000 Secrets,** Addison Wesley, Boston, 2001.