Bilgisayarlar İçin Bağışıklık Sistemi

Herhangi bir özelliği olmayan ve içinde sıra sıra PC'lerin bulunduğu küçük penceresiz bir oda. Ama görünüş aldatıcı olabilir. Burası, hanta veya Ebola gibi öldürücü virüsler üzerinde çalışmaların yürütüldüğü yüksek güvenlikli bir mikrobiyoloji laboratuvarının eşdeğeri olan bir bilgisayar laboratuvarı. Çok bulaşıcı virüsler taşıyan yüzlerce disket, bir kısmı tezgahların üzerine yığılmış bir kısmı yarı açık çekmecelere tıkıştırılmış vaziyette duruyor. IBM'in NewYork Hawthorne'daki Watson Araştırma Merkezi'nde yer alan virüs ayırma laboratuvarında 12 000 dolayında bilgisayar virüsünün yanısıra bunları saptayan, güvenilir bir şekilde ayıran ve yok eden donanım bulunuyor.

Jeffrey Kephart, şirketin AntiVirus logosunu gösteren büyük ekranlı bir monitörün önünde oturuyor. IBM AntiVirus; birçok virüsle mücadele yazılımından yalnızca biri. Ama Kephart'ın büyük planları var; ortaya çıkabilecek siberuzay hastalıklarından bizleri koruyacak küresel bir bağışıklık sistemi yaratmaya çalışıyor. "İnsan soyunun varlığını sürdürmesinin tek nedeni bir bağışıklık sisteminin varlığıdır" diyor Steve White ve ekliyor "Siberuzayın varolabilmesi de sahip olacağı bir bağışıklık sistemi sayesinde olacaktır."

Kephart, White ve çalışma arkadaşları, araştırma yazılarında bilgisayar ağları ile canlı organizmalar arasındaki çarpıcı benzerlikleri vurguluyorlar. Elektronik organizmaları tehlikeli yeni bulaşıcı hastalıklardan koruyabilmek için epidemiyoloji ve immünolojinin yaklaşımlarından faydalanılabileceğini iddia ediyorlar. Hatta bu düşüncelerini bir IBM bilgisayar ağı üzerinde denemeye almışlar ve bu yılın sonlarında bağışıklık sistemlerinin bir bölümünü halka açmayı planlıyorlar.

Bilgisayar virüsleri, bilgisayarınıza gizlice girmek, kendilerinin benzerlerini üretmek ve diğer bilgisayarlara yayılmak amacıyla tasarlanmış sinsi programlardır ve genellikle birkaç belirtiye neden olurlar. Bu belirtiler, sisteminizin yavaşlaması ya da anlaşılamaz bir biçimde dokümanlarınızda "Wazza" sözcüğünün görünmesi şeklinde olabilir. Ya da zatürrenin sayısal bir karşılığı gibi olabilir -bazı virüsler doğrudan sabit diski tahrip ederler.

Geçmişte virüsler bir bilgisayardan diğerine disketler aracılığıyla taşınıyorlardı. Bilgisayarınızı virüslü bir disket üzerinden açarsanız ya da disketteki virüslü bir programı çalıştırırsanız virüs bilgisayarınızın belleğinin bir bölümünü ele geçirir ve kendini diğer dosyaların içine kopyalamaya başlar. Bu kopyalama işlemi bilgisayarınızda kullandığınız disketlere de uygulanır ve temiz disketlerinize de artık virüs bulaşmış olur.

Virüs tehdidine karşı mücadele veren ve bilgisayarınızı virüs bulaşmasına karşı koruyacağı iddiasındaki yazılımları satan büyük bir endüstri gelişmektedir. Bu antivirüs sistemlerinin çoğunun temelinde bir virüs tarayıcı (scanner) bulunuyor. Bu da bilgisayarınızın belleğindeki bütün kodlarda, bilinen virüslerin "işaret"lerini arayan bir teşhis programı. İşaret ise ufak bir kod parçası. Antivirüs sisteminin yaratıcısı tarafından özenle belirlenmiş olan bu kod parçası normal programlarda kesinlikle bulunmaz ancak ilgili virüsün temel bir parçası. Eğer tarayıcı bu işareti saptarsa sizi uyarır.

Bu sistemin sorunu sürekli olarak yeni virüslerin yaratılması. Her sekiz günde yeni bir virüsün ortaya çıktığı tahmin ediliyor ve bu hız giderek artıyor. Bu durumda antivirüs yazılımı üreten firmalar sürekli yeni virüslerin peşinden koşturuyorlar. Yeni bir virüs tespit ettiklerinde yalnızca o virüste bulunan işareti ortaya çıkartarak kendi yazılımlarına dahil ederler ve birkaç ayda bir yazılımın güncelleştirilmiş sürümü piyasaya sürülür. Ancak bu yazılımlar virüslerin çoğalma hızına erişemediklerinden daha dağıtılmaya başladığı gün güncelliklerini yitirmişlerdir.

Yine de bu sistemin şimdiye kadar oldukça iyi işlediği söylenebilir. Birçok virüs birkaç bilgisayardan öteye yayılmaz. White'ın dediğine göre ya zamanında farkedilirler ya da yeterince etkili değildirler. Öte yandan bazıları da öyle yıkıcı olurlar ki daha yayılma fırsatı bulamadan içinde bulundukları bilgisayarı kullanılmaz hale sokarlar. Ama bazı başarılı virüsler de yıllar içinde tüm dünyaya yayılırlar.

Ancak bilgisayar ağlarındaki makro virüsler diye adlandırılan yeni bir virüs ailesi ile birlikte herşey değişiyor. Artık virüsler, makroların -Microsoft Word ya da Excel gibi programlarla yazılan dökümanlara iliştirilen küçük program parçaları- içine gizleniyorlar. Bu dokümanlardan herhangi birini açtığınız zaman virüs bilgisayarınıza bulaşır. Carlisle, Pennslyvania'da bulunan Ulusal Bilgisayar Güvenlik Kurumu (National Computer Security Association) tarafından yapılan bir araştırmaya göre bugünlerde en büyük sorunlar Concept adlı bir makro virüsten kaynaklanıyor. Disketlere yayılabildiği gibi e-mail'lerle, WWW'den ve ilan tahtalarından alınan dosyalarla da dolaşıyor. Bilgisayar

ağlarını kullanan bu makro virüsler birkaç hafta içinde de tüm dünyaya yayılabiliyor.

"Uçağın bulunmasıyla hastalıkların çok daha hızlı yayılması gibi Internet nedeniyle de bilgisayar virüsleri disketleri kullandıkları döneme göre çok daha hızlı yayılmaktadırlar. Internet ve diğer küresel ağları kullananların sayısı her geçen gün artmaktadır ve mevcut antivirüs yöntemleri de yetersiz kalmaya başlayacaktır" diyor White. Yeni virüsler öyle hızlı yayılıyor ki araştırmacılar virüsün işaretini çıkartıp güncel antivirüs yazılımını gönderinceye kadar ciddi hasarlar meydana gelebiliyor. Açıkçası bilgisayar ağlarını koruyabilmek için daha hızlı işleyen bir yönteme gereksinim var.

IBM araştırma ekibi böyle bir korunma yöntemi geliştirmek için doğal yaşamdan esinlenmeye yönelmiş. Ancak bilgisayar virüsleri yapay bir yaşamın yapıları. "Onları virüs olarak adlandırmak yerindedir." diyor White. Onlar da aynen biyolojik virüslerin yaptığı gibi kendi benzerlerini üretmek için ev sahiplerinin kaynaklarını kullanırlar . "Analoji nefes kesici bir derinlik ve önem taşır." Ekip daha sonra bağışıklık sisteminin insanları nasıl koruduğunu incelemiş. Bir düzeyde, bağışıklık sistemimiz vücutta rastladığı insana ait olmayan herşeyi imha etmektedir. Ancak bu strateji bilgisayar virüsleri ile mücadele için uygun değil. Çünkü zaman içinde hemen hemen tüm kullanıcılar bilgisayarlarına yeni yazılımlar yükleyecekler ya da eskilerini güncelleştireceklerdir. Yeni yazılımlara otomatik olarak saldıracak şekilde tasarımlanan bir bağışıklık sistemi, açıktır ki kendinden beklenilen işlevi yapamayacaktır.

Ancak biyolojik bağışıklık sistemlerinin daha özel tepkileri de var. Vücuda yabancı bir organizma (mikrop, virüs) girdiğinde bunu tespit edip ortadan kaldıracak antikorlar üretilmeye başlanır. Bağışıklık sistemi, patojeni tamamen analiz etme gereği duymaz. Virüsün yapısı hakkında onu ilerde tanıyacak kadar bilgi sahibi olması yeterlidir. İlk enfeksiyon atlatıldıktan sonra bu virüs ile mücadele eden antikorlardan bir kısmı vücutta muhafaza edilir. Böylece aynı virüs ile ilerde tekrar karşılaşıldığında çok daha hızlı bir savunma yapılabilecektir.

Kasıtlı Bulaştırma

Bunlar tümüyle mevcut antivirüs programlarının yaptıklarına benzemektedir. Yazılım sistemi antikorlar içerir ve bu antikorlar bir bütün olarak virüsleri değil de onların belirtilerini tanırlar. White, Kephart ve arkadaşlarının yapmış oldukları da bu analojiyi biraz daha ileri götürerek virüs tespit işlemini hızlandırmak ve bunu tek bir bilgisayar için değil, birçok bilgisayar içeren ağlar için genişletmektir.

Virüs ayırma laboratuvarında Kephart stratejilerini açıklıyor. Önce bir bilgisayarın "temiz" olduğunu anlamak için AntiVirüs'ü çalıştırıyor. Sonra virüslü bir disketi alıyor. Sürücüsüne yerleştirip bilgisayara virüs bulaştırıyor ve tekrar AntiVirüs'ü çalıştırıyor. Seçmiş olduğu virüs, sistemin daha önceden bildiği bir virüs değil ve tarayıcı program bu virüsün işaretini bilmediği için tespit edemiyor. Ancak yazılımın diğer bir kısmı -bütünlük kontrolcüsü- birşeylerin yanlış olduğunu farkediyor. Kontrolcü, bilgisayardaki tüm programları teker teker tarayarak en son çalıştırıldıkları halleriyle karşılaştırıyor ve eğer bir fark bulursa alarm veriyor.

Farklılığın nedeni bir virüsün varlığıysa antivirüs yazılımı hasarı onarabilir. Bunu da herhangi bir virüsün kendisini bilgisayara yerleştirmek ve programları bozmak için kullanacağı olası yöntemleri gözönüne alarak yapar. Eğer yazılım, virüsün yapmış olduğu hasarı onarabilirse dosyalar eskisi gibi çalışırlar. Ama başarı garantisi her zaman yoktur.

Bütün bunlar antivirüs programlarının yıllardır zaten yapageldiği şeylerdir. Her ne kadar bilgisayardaki bozuk dosyalar onarılmış olsa da virüs yeni tahribatlar için hazır bir şekilde beklemektedir. Yeni bir virüsü tespit edip ortadan kaldırabilmek için koruyucu yazılımın o virüsün işaretine gereksinimi vardır. Daha da kötüsü, bir yerlerde konunun uzmanı olan bir programcının virüsü yakalayıp yapısını inceleyerek işaretini ortaya çıkarmasına kadar herhangi bir şey yapılamaz. White ve Kephart'ın deneysel bağışıklık sistemi bu sorunlar üzerinde birşeyler söyleyecek durumda. Virüs bulaşmış bilgisayar yeni virüsün içinde gizlendiği dosyayı saptadıktan sonra bunu şifreleyip IBM'in merkezi virüs çözümleyicisine gönderir. Ağ üzerinden IBM'e gönderme işlemi bilgisayar tarafından otomatik olarak yapılabildiği gibi kullanıcının veya bilgisayar ağında ağ yöneticisinin kontrolünde de yapılabilir.

Laboratuvar gösteriminde virüs çözümleyici ile virüslü bilgisayar yan yana duruyor. Bilgisayarda kullanıcılardan birinin göndermiş olduğu bir virüs bulunuyor. Çözümleyici önce gönderilmiş olan programın şifresini açar ve bilinen virüsler arasında olup olmadığını görmek için bilgisayarı taramaya başlar. Ancak Kephart'ın çözümleyicisi virüsü tanıyamaz; yepyeni bir virüsle karşı karşıyadırlar.

Şimdi çözümleyici, virüsün kendi kendisini ortaya çıkartması için çalışmaya başlar. Bilgisayarın içine virüs üzerinde güvenle çalışabilecek bir "sanal bilgisayar" kurulmuştur. Sanal bilgisayar da gönderilen programı çalıştırmış ve virüslenmiştir. Ayrıca bu

sanal bilgisayara virüsün ilgisini çekebilecek yem programlar yerleştirilmiştir. Ve bu programlar -virüsün harekete geçip marifetlerini ortaya koyması amacıyla- çalıştırılır, okutulur, yazdırılır, kopyalanır vs.

İz Peşinde

Herbir işlemden sonra çözümleyici, yem programların son durumlarını ilk durumlarıyla karşılaştırarak virüsün nasıl bir etkisi olduğunu inceler. Bu yolla virüsün programlara nasıl girdiğini ve onları nasıl bir değişikliğe uğratarak gizlendiğini ortaya çıkartır. Bu bilgi daha sonra uzaktaki, virüslü kullanıcıya gönderilir ve virüsü etkisiz hale getirip yapmış olduğu hasarı onarmak için kullanılır.

Çözümleyicinin bir sonraki işi, virüs için bir işaret saptayıp uzaktaki kullanıcının antivirüs yazılımına göndermek ve onun gelecekte bu virüsü rahatça tespit edebilmesini sağlamaktır. Virüslerden işaret çıkartmak ustalık isteyen bir iştir ve şimdiye kadar hep insanlar tarafından yapılagelmiştir. "Gizli ve herkesin bilmemesi gereken bir beceridir. Hemen hemen başka hiçbir işe de yaramaz" diyor White. Kodlarının yaşamsal olmayan kısımlarında meydana gelen farklılıklarla virüsler sık sık değişime uğrarlar. Bu nedenle seçilecek işaret, virüsün esasını oluşturan kod parçalarından çıkartılmalıdır. Tabii ki bu da normal yazılımlarda kesinlikle yer almayacak bir kod parçası olmalıdır. Aksi takdirde antivirüs programları oldukça pahalı yazılımlara saldırıp hasar verebilirler. Virüs avcısı uzmanlar virüslerin çalışma mekanizmalarında yer alan temel kod parçalarını tanımayı öğrenmiş kişilerdir.

Ama IBM araştırma ekibi bu işi de artık bilgisayarların üstlenmesi gerektiğini düşünüyor ve bunun üzerinde çalışıyor. Ancak bir insanın görüş yeteneğine sahip bir programı henüz yazamadıkları için bu konuda bilgisayarların en iyi yapabildiği şey -büyük miktarlarda sayısal karşılaştırma yapma- üzerinde yoğunlaşmış durumdalar. Kephart ve White'ın otomatik işaret çıkartıcısı, pekçok gigabayt yer tutan onbinlerce programın kodlarını yeni virüsün koduyla karşılaştırıp herhangi bir yasal programda bulunmayan ve işaret olabilecek kısa komut parçaları aramaktır. Bu işi de oldukça iyi yapmaktadır. IBM'deki testlerde insanlardan daha iyi bir performans göstermiştir. Sonunda virüs çözümleyici, uzaktaki sorunlu bilgisayara virüsün işaretini ve hasarı onarma komutlarını göndereceğini bildirir.

Kephart'ın gösterisi yaklaşık bir dakika sürüyor. Ancak o ve White daha da ileri gitmeyi amaçlıyorlar. Plan-

larının ilk aşamasında IBM'in WWW adresine (http://av.ibm.com) giren herkesin yeni virüsün işaretini ve gerekli hasar onarım komutlarını alabilmeleri var. "Kullanıcılar hergün, her saat yeni işaretler alabilecekler" diyor Kephart.

Daha da hızlı bir korunma sağlamak için iki araştırmacı tüm bu süreci otomatik hale getirmek istiyorlar. Böylece dünyanın her tarafından virüslü bilgisayarlar yeni virüs örneklerini doğrudan IBM virüs çözümleme merkezine gönderecekler. Burada gerek virüslerin tespit ve imha edilmelerinde kullanılan yeni yöntemler gerekse yarattıkları hasarın onarılması için yapılacak çalışmalar otomatik olarak gerçekleştirilecek. Bunlar virüslü kullanıcılara geri gönderileceği gibi dünyadaki diğer tüm kullanıcıların da yararlanması sağlanacak. Kephart ve White, tedavinin dağıtılma hızının virüsün yayılma hızının önüne geçmesi sayesinde tüm sistemin salgından korunabileceğini umuyorlar. "Herşey çok kısa bir zaman diliminde gerçekleşeceğinden bütün dünya korunmuş olacak" diyor Kephart.

IBM bu bağışıklık sisteminin pilot uygulamasını bir grup şirket üzerinde bu yılın sonunda başlatacak. Projenin tamamının da kısa bir süre sonra devreye alınması bekleniyor. Eğer tüm siberuzay yakın bir gelecekte IBM'in bağışıklık sistemi tarafından korunursa rakip antivirüs firmaları ne yapacaklar? Onlar da kepenklerini henüz indirmiş değiller. Jimmy Kuo, California'daki McAfee Associates'te görevli bir virüs araştırmacısı. Onların da kendi antivirüs yazılımları var. Ağ ve makro virüslerin çok daha hızlı yayılıyor olduklarını ve araştırmacıların işlerinin zorlaştığını Kuo da kabul ediyor. Ayrıca McAfee ve rakipleri de IBM'in bağışıklık sistemine benzer yazılımlar kullanmaktalar. Kuo, bir otomatik sistemin herşeyiyle kendi kendine işleyebilecek kadar geliştirilebileceğini kabul etmiyor. "Bir hedef olarak güzel" diyor Kuo "ama virüs bilgisiyle donanmış bir insanın sonuçları gözden geçirmesi çok daha iyi olacaktır."

NCSA'dan Donathan Wheat ise IBM'in sisteminde daha büyük potansiyel görüyor -özellikle hasar meydana gelmeden önüne geçme ve onarımları en kısa zamanda gönderme konusunda. "Makro virüsler yeni bir dönemi açıyorlar" diyor Wheat. Yazılmaları kolay, herhangi bir programlama becerisi gerektirmiyor ve sayıları da hızla artıyor. Önlerini kesecek otomatik sistemler olmadıkça sonuçları korkunç olabilir. "Sonunda" diyor Wheat "kontrolden çıkılmış bir noktaya gelinebilir".

Kurt Kleiner,
The Internet Strikes Back, New Scientist, 24 Mayıs 1997
Çeviri: Çağlar Sunay