Bilgisayarınıza Güvenebilir Misiniz?

Yazan:
Richard M. Stallman
<rms (at) gnu.org>

Çeviren:
Doruk Fişek
<dfisek (at) fisek.com.tr>

Hazırlayan:
Deniz Akkuş
<deniz (at) belgeler.org>

Ocak 2003

Özet

Makalenin özgün sürümünü http://www.gnu.org/philosophy/can-«you-«trust.html adresinde bulabilirsiniz.

Bilgisayarınız emirlerini kimden almalı? Çoğu insan kendi bilgisayarının başkalarına değil kendisine itaat etmesi gerektiğini düşünür. "Güvenilir bilgi işlem" adı verdikleri bir planla büyük medya kuruluşları (film ve müzik firmaları dahil), Microsoft ve Intel gibi bilgisayar firmaları ile işbirliği yaparak bilgisayarınızın size değil kendilerine itaat etmesini hedefliyorlar. Sahipli programlar daha önce de art niyetli özellikler içermişti, ancak bu plan bunu evrensel yaygınlığa kavuşturuyor.

Temel olarak sahipli yazılımlar, yazılımın ne yaptığını kontrol etmenize, kaynak kodunu incelemenize ya da değiştirmenize izin vermezler. Zeki işadamlarının yazılım üzerindeki bu mutlak hakimiyetlerini sizin aleyhinize kullanmaları için çeşitli yollar geliştirmeleri şaşırtıcı olmasa gerek. Microsoft, daha önce bunu defalarca yaptı: Windows'un bir sürümü Microsoft'a sabit diskinizde kurulu tüm yazılımları bildirmek için tasarlanmıştı; Windows Media Player'ın yakın zamanda çıkan bir "güvenlik" güncellemesi kullanıcıların yeni bazı kısıtlamaları kabul etmesini şart koşuyor. Ama Microsoft yalnız değil: KaZaa müzik paylaşma programı, KaZaa'nın iş ortağının müşterilerine sizin bilgisayarınızın kullanımını kiralayabilmesine uygun tasarlanmıştı. Bu art niyetli özellikler çoğu zaman gizlidir, ama bir kez farkettiğiniz zaman da onları ortadan kaldırmak zordur, çünkü elinizde kaynak kodu yoktur.

Geçmişte bunlar istisnai olaylardı. "Güvenilir bilgi işlem" bunun kaide haline gelmesini sağlayacaktır. "Hain bilgi işlem" bu sistemler için daha uygun bir isim, çünkü bu plan bilgisayarınızın sizin emirlerinize uymamasını sağlamayı hedeflemektedir. Bu sistemler, bilgisayarınızın genel amaçlı bir makina olmasını engeller ve bilgisayarınızın yapacağı her işlem için başkalarından izin ister hale gelmesini sağlayabilir.

Teknik olarak hain bilgi işlemin altyapısı, bilgisayarın içinde dijital bir şifreleme ve imzalama aygıtının olması ve anahtarlarının sizden saklanmasına dayanır (buna Microsoft'un verdiği isim: "palladium"). Sahipli yazılımlar bu aygıtı hangi programları çalıştırma izniniz olduğunu, hangi belge ya da bilgilere ulaşma izniniz olduğunu ve bu belge ve bilgileri hangi programlara aktarma izniniz olduğunu kontrol etmek için kullanacak. Bu programlar düzenli olarak Internet aracılığıyla yeni izin verme kuralları indirecek ve size bunu otomatik olarak uygulayacak. Eğer bilgisayarınızın yeni kuralları periyodik olarak Internet'den indirmesine izin vermezseniz, bazı işlevleri kullanılamaz hale gelecek.

Elbette, Hollywood ve plak şirketleri hain bilgi işlemi "DRM" (Dijital Kısıtlamalar Yönetimi) için kullanmayı planlıyor, böylece indirilen video görüntüleri ve müzik sadece belirlenen tek bir bilgisayarda izlenebilecek/çalınabilecek. Bu

şirketlerden satın alacağınız izinli dosyaları paylaşmanız tamamen imkansız hale gelecek. Siz, toplum olarak, dosyalarınızı paylaşabilme özgürlüğüne ve yeteneğine sahip olmalısınız. (Ben birisinin şifrelenmemiş sürümleri üretmenin, onları gönderme ve paylaşmanın bir yolunu bulacağını, böylece DRM'nin tam olarak başarılı olamayacağını tahmin ediyorum, ama bu ümit, planlanan sistem için bir mazeret olamaz).

Paylaşımı imkansız hale getirmek yeterince kötü, ama daha da kötüsü var: Aynı sistemi e–posta ve belgeler için de kullanma planları mevcut. Bunun sonucu olarak iki hafta içinde yok olan bir e–posta ya da sadece belirli bir şirketin bilgisayarlarında okunabilen belgeler oluşturmak mümkün olacak.

Düşünün ki patronunuzdan riskli olduğunu düşündüğünüz bir şeyi yapmanızı emreden bir e–posta aldınız; bir ay sonra, yapılan iş geri teptiğinde, emir altında hareket ettiğinizi göstermek için e–postayı kullanamıyorsunuz. Uçan mürekkeple yazılan emri "yazılı olarak almak" sizi korumayacak.

Düşünün ki patronunuzdan yasadışı ya da etik olmayan şeyler yapmanızı isteyen, örneğin şirketinizin denetim raporlarını kağıt öğütücüden geçirmenizi isteyen ya da ülkeniz için ciddi bir tehdidin kontrolsüz ilerlemesine izin vermenizi isteyen bir e–posta aldınız. Bugün bunu bir muhabire gönderebilir ve olayı ortaya çikarabilirsiniz. Hain bilgi işlem dünyasında, muhabir belgeyi okuyamayacaktır, çünkü bilgisayarı onun emirlerini dinlemeyecektir. Hain bilgi işlem, yozlaşma için bir cennet olacaktır.

Microsoft Word gibi kelime işlemciler, rekabet ettikleri başka kelime işlemciler açamasın diye belgelerinizi kaydederken hain bilgi işlemi kullanabilirler. Bugün, Word belgelerini okuyan özgür kelime işlemciler geliştirebilmek için word dosya biçeminin sırlarını uzun süreli deneme yanılma çabaları ile buluyoruz. Eğer Word, belgenizi kaydederken hain bilgi işlemi kullanarak şifreleme yaparsa, özgür yazılım topluluğunun o belgeyi okuyacak bir program geliştirme şansı bile olmayacaktır – geliştirmeyi başarsak bile, böyle programlar DMCA (Dijital Çağ Telif Hakkı Yasası) nedeniyle yasaklanabilecektir.

Hain bilgi işlem kullanan programlar, Internet'den sürekli yeni kurallar indirecek ve otomatik olarak bu kuralları çalışmalarınıza empoze edecektir. Eğer Microsoft ya da Amerikan hükümeti, yazdığınız bir belgede söylediklerinizi beğenmezse tüm bilgisayarlara yeni bir talimat göndererek sizin belgenizi kimsenin okumasına izin vermeyebilir. Yazınız 1984 romanındaki gibi geriye yönelik olarak iz bırakmaksızın kaybolacaktır. Kendi yazınızı siz bile okuyamayabilirsiniz.

Hain bilgi işlemin yapacağı çirkin eyler hakkında bilgi edinebilir, bunların ne kadar etkili/önemli olabileceini inceleyebilir ve bunu kabul edip etmemeye karar verebilirsiniz. Hain bilgi işlemi kabul etmek dar görüşlü ve aptalca olur ama esas önemli olan nokta, yaptığınızı düşündüğünüz anlaşmanın durağan olmamasıdır. Bir kez programı kullanmaya bağımlı hale geldiğiniz anda oltaya takılmış durumdasınız ve onlar bunu biliyorlar; artık anlaşmayı değiştirebilirler. Bazı uygulamalar otomatik olarak güncellemelerini indirecek ve bir şeyleri farklı yapmaya başlayacaklar – ve güncelleme ya da güncellememe seçeneğini size sunmayacaklardır.

Bugün sahipli yazılımlarla kısıtlanmaktan, onları kullanmayarak kaçınabilirsiniz. GNU/Linux ya da başka bir özgür işletim sistemi kullanırsanız ve üzerine sahipli programlar kurmaktan kaçınırsanız, bilgisayarınızın ne yaptığına siz karar verirsiniz. Eğer özgür bir programın art niyetli bir özelliği varsa, diğer programcılar bunun farkına vararak düzeltebilir ve siz de programın düzeltilmiş halini kullanabilirsiniz. Özgür olmayan işletim sistemlerinde de özgür programlar ve araçlar kullanabilirsiniz; bu size tamamen bir özgürlük sağlamayı başaramasa da birçok kullanıcı böyle yapıyor.

Hain bilgi işlem özgür işletim sistemlerinin ve özgür uygulamaların varlığını tehdit ediyor, çünkü özgür sistemleri çalıştırmanız bu yolla engellenebilir. Hain bilgi işlemin bazı biçimleri, işletim sisteminin belirli bir şirket tarafından onaylanmış olmasını gerektirecek. Bazı biçimleri, işletim sistemi üzerinde çalıştıracağınız her programın işletim sisteminin geliştiricisi tarafından onaylanmasını zorunlu kılacak. Böyle sistemlerde özgür yazılımları çalıştıramazsınız. Bu sistemleri bertaraf etme yollarını bulmanız ve başkalarına açıklamanız ise suç addedilecek.

Amerika'da şimdiden tüm bilgisayarların hain bilgi işlemi desteklemesini zorunlu kılan ve eski bilgisayarların da internete bağlanmasını engellemeye yönelik yasa teklifleri bulunuyor. CBDTPA (biz ona Tüket Ama Pro-

gramlamaya Çalışma Yasası diyoruz) bunlardan biri. Hain bilgi işlem kanun zoru ile uygulanmasa bile, kabul görmesi için büyük bir baskı oluşturulabilir. Bugün insanlar çok çeşitli sorunlara yol açmasına karşın (http://www.gnu.org/philosopy/no-«word-«attachments.html) iletişim için sıkça Word biçimini kullanmakta. Eğer son sürüm Word belgeleri sadece hain bilgi işlem içeren bilgisayarlar tarafından okunabilir şekile getirilir ve kullanıcılar salt bireyci bir yaklaşımla hareket ederse, pek çok kişi hain bilgi işleme geçecektir. Hain bilgi işlemle mücadele edebilmek için birlik olmalı ve kollektif bir harekette bulunmalıyız.

Hain bilgi işlem ile ilgili daha fazla bilgi için, bakınız http://www.cl.cam.ac.uk/users/rjal4/tcpa-«faq.html.

Hain bilgi işlemi engellemek, organize bir hareket gerektirecek. Sizin yardımınıza ihtiyacımız var! Electronic Frontier Foundation (http://www.eff.org/ — Elektronik Serhat Vakfı) ve Public Knowledge (http://www.publicknowledge.org/ — Kamu Bilgisi) hain bilgi işleme karşı kampanyalar düzenliyor – tıpkı Free Software Foundation'ın (Özgür Yazılım Vakfı) sponsorluğunu yaptığı Dijital İfade Projesi (http://www.digitalspeech.org/) gibi. Lütfen çalışmalarına destek olabilmek için bu web sitelerini ziyaret edin.

Intel, IBM, HP/Compaq ya da bilgisayarınızı aldığınız firmanın halkla ilişkiler bölümlerine "güvenilir"(!) bilgisayar sistemleri almaya zorlanmak istemediğinizi ve onların bu tür sistemleri üretmemelerini istediğinizi yazarak da yardımcı olabilirsiniz. Bu eylem tüketici gücünün baskısını arkamıza almamızı sağlayabilir. Eğer bunu bireysel olarak yaparsanız, mektuplarınızın birer kopyasını lütfen yukarıdaki kuruluşlara (EFF[B7], PK[B8]) gönderin.

Dipnotlar:

1. GNU Projesi, genel/özel anahtar metodu ile şifreleme ve dijital imzalama yapılmasını sağlayan GNU Privacy Guard'ı (GNU Mahremiyet Koruyucusu – GPG) dağıtmaktadır. Bu yazılımı kullanarak özel e–postalarınızı güvenli şekilde gönderebilirsiniz. GPG'nin hain bilgi işlemden nasıl farklı olduğunu incelemek, birini faydalı, diğerini ise tehlikeli yapanın ne olduğunu görmek için yararlıdır.

   Birisi GPG kullanarak şifrelenmiş bir belge yolladığında ve siz onu GPG kullanarak açtığınızda, sonuç olarak elde ettiğiniz şifresiz belgeyi okuyabilir, yönlendirebilir, kopyalayabilir ve hatta tekrar şifreleyerek güvenli olarak bir başkasına yollayabilirsiniz. Bir hain bilgi işlem uygulaması, sizin yazıları ekranda okumanıza izin verir ama başka işler için şifresiz bir belge üretmenize izin vermez. GPG, bir özgür yazılım paketi olarak güvenlik özelliklerini kullanıcıların hizmetine sunar; kullanıcılar GPG'yi kullanırlar. Hain bilgi işlem kullanıcılara kısıtlamalar empoze etmek için tasarlanmıştır, hain bilgi işlem kullanıcıları kullanır.

2. Microsoft, Palladium'u bir güvenlik önlemi olarak pazarlıyor ve virüslere karşı koruma sağlayacağını iddia ediyor ama bu iddia açık olarak yanlış. Microsoft Research tarafından Ekim 2002'de yapılan bir sunumda Palladium'un özelliklerinden birinin, mevcut işletim sistemlerinin ve uygulamalarının çalışmaya devam edecek olması olduğu belirtildi; bu da virüslerin bugün tüm yapabildikleri şeyleri yapmaya aynen devam edecekleri anlamına geliyor.

   Microsoft "güvenlik"ten Palladium ile bağlantılı olarak bahsettiğinde, normalde bu kelimenin karşılığı olan "makinanızı istemediğiniz şeylerden korumak" anlamında kullanmıyorlar. Sizin, verilerin makinanızda bulunan kopyalarına, başkalarının istemediği şekillerde ulaşmanızdan korumayı kastediyorlar. Sunumdaki bir slayt, Palladium'un korumak için kullanılabileceği çeşitli sır tiplerini listeliyordu. Bunların arasında "üçüncü kişilerin sırları" ve "kullanıcı sırları" vardı. Ama "kullanıcı sırları" tırnak içine alınmıştı — çünkü bu Palladium'un ana tasarım amacı değildi.

   Sunumda güvenlik konusu ile sıkça ilintilendirdiğimiz diğer terimlere de yer verildi — "saldırı", "art niyetli kod", "spoofing", "güvenilir". Hepsine yeni anlamlar yüklenmişti: "Saldırı" birisinin size zarar vermeye çalıştığı anlamına gelmiyor, müzik kopyalamaya çalıştığınız anlamına geliyor. "Art niyetli kod", başkalarının istemediği bir işi makinanıza yaptırabilmek için sizin yüklediğiniz yazılım manasına geliyor. "Spoofing" bir başkasının sizi kandırmaya çalışması değil, sizin Palladium'u kandırmaya çalışmanız anlamına geliyor. Ve berdevam...

3. Palladium geliştiricileri tarafından daha önce verilen bir demeçte sistemin temel dayanak noktası olarak, her kim bilgiyi geliştirmiş ya da toplamış ise nasıl kullanacağı konusunda da tam kontrole onun sahip olması esasının alındığı ifade ediliyor. Bu süregelen etik fikirlerin ve yasal sistemin bir ihtilal ile alaşağı edilmesi ve bir benzeri daha bulunmayan bir kontrol sisteminin oluşturulması demektir. Bu sistemlerin kullanımı ile öngördüğümüz problemler bir kaza eseri değildir; temel amacından kaynaklanmaktadır. Reddetmemiz gereken şey, kontrolü bizden alıp başkalarına devreden bu temel amaçtır.

Notlar

a) Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

b) Konsol görüntüsünü temsil eden sarı zeminli alanlarda metin genişliğine sığmayan satırların sığmayan kısmı ¬ karakteri kullanılarak bir alt satıra indirilmiştir. Sarı zeminli alanlarda ¬ karakteri ile başlayan satırlar bir önceki satırın devamı olarak ele alınmalıdır.

(B7) http://www.eff.org/

(B8) http://www.publicknowledge.org/

Bu dosya (bilgisayariniza–guvenebilir–misiniz.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

18 Şubat 2007