Trusted Computing ve Linux

Bora Güngören
Portakal Teknoloji
bora@portakalteknoloji.com
Akademik Bilişim 2006
09.02.2006

Sunum Planı

- Güven Kavramı
- Güvenilir Bilişim (Trusted Computing)
- DRM ve TCPA'e Tepkiler
- Güvenilir İşletim Sistemi (Trusted OS)
- Microsoft Vista
- Trusted Linux
- Open Trusted Computing

Güven Kavramı

- Güven kavramını nasıl tanımlamalıyız?
  - Birisinin davranışlarının beklentilerimize göre şekilleneceğinden emin olmamız durumunda o kişiye güveniriz.
- Karşılıklı güven sağlanması için
  - Önceki deneyimlere dayanan ilişki
  - Zaten güvenilen bir üçüncü kişinin garantisi
- Güven ilişkilerinin çoğunluğu “kesinlikle güvenilen” (absolute trust) bir yerin doğrulamasına ihtiyaç duyar.
  - Bu üçüncü yere “güvenin kökeni” (root of trust) adı verilir.

Güven Kavramı

- Günlük yaşamımızda “devlet” bizim için bir güven kaynağıdır.
- Devletin parçası olan kurumların çeşitli etkinlikleri ile kendimizi güvende hissederiz
  - Kimlik ve gerçekliğin doğrulanması (soğuk damgalı kimlikler, sahte paranın engellenmesi)
  - Yetkilendirme (noter onaylı imza örnekleri)
  - İstenirse bilginin gizli tutulması (118'deki kaydın silinmesi)
  - Bilgilerin üçüncü kişilerce değiştirilmemesi (durduk yerde sabıka kaydımız değişmez)
  - Bilgilere erişimin garantilenmesi (aslı gibidir onaylı kopya temini)
  - Bilgilerin yeniden sağlanabilmesi (kaybolan kimliğin yerine yenisini almak)

Güven Kavramı

- Güven ilişkisini, mal, para ve bilgi akışının “güven” duygusu içerisinde sağlanmasına dayandırmamız gerekir.
- Temel olarak güven ilişkisi aşağıdaki dört bileşenden oluşur:
  - Gizliliğin sağlanması (confidentiality)
  - Bütünlüğün sağlanması (integrity)
  - Erişimin sağlanması (availability)
  - Kurtarmanın sağlanması (recoverability)

Güvenilir Bilişim (Trusted Computing)

- Güvenilir Bilişim (Trusted Computing) 1990'ların sonundan itibaren ortaya çıkan çok sayıda güvenlik odaklı problemin çözümü için son 3-4 yıl içinde getirilen bir yaklaşımın adıdır.
  - Virüs ve solucanlar
  - İstenmeyen eposta (spam)
  - Uygulamaların kırılması
- Güvenilir Bilişim, bilişim sistemlerini oluşturan bileşenlerin her biri arasında az önce saydığımız dört temel gereksinime dayanan bir “güven ilişkisi” planlar.
  - Bu ilişkiler sağlanırsa çok değişik güvenlik sorunları kolayca engellenebilir.

Güvenilir Bilişim (Trusted Computing)

- Bu ilişkilerin de bir “kökeni” olması gerekir. O zaman bu kökeni nasıl sağlamalıyız?
- Kökeni sağlayacak olan bileşenin
  - Kendisinin diğer bileşenlerden bağımsız olması
  - Kendisinin kurcalanmasının ve bozulmasının engellenmesi
- Yazılım bileşenleri tek başlarına köken olamazlar. Kökenin donanım olması gerekir.
  - Bu donanım bilgisayar açıkken ve kapalıyken aktif olmalıdır.
  - “Elektriksel” saldırılardan etkilenmemelidir.

Güvenilir Bilişim (Trusted Computing)

- Trusted Platform Module (TPM) bu güvenin kökeni olacak donanım için bir tanımlamadır.
  - Tanımlama Trusted Computing Group (TCG) tarafından yayınlanmıştır.
- İsteyen her donanım üreticisi TPM üretebilir.
  - TPM özelliği ayrı bir entegrede olabilir (Infineon, Atmel, National)
  - TPM işlemciye entegre olabilir (Crusoe, Intel LaGrande, AMD Pacifica)
  - TPM ana karttaki başka bir entegrenin içine gömülebilir (Broadcom Gigabit Ethernet)
  - TPM özellikle güvenilir olmak isteyen bir donanımda ayrıca bulunabilir. (Seagate'in bazı prototip diskleri)

Güvenilir Bilişim (Trusted Computing)

- Bir TPM bize ne sağlar?
  - 2048 bit RSA ile açık anahtar altyapısı (anahtar oluşturma, saklama, anahtar işlemleri)
  - Simetrik anahtar altyapısı
  - MD-5 ve SHA-1 ile özetleme
  - Gerçek rastgele sayı üreticisi (TRNG)
  - Yönetim işlevleri
- Ayrı bir TPM entegresi çok ucuzdur 2-3 Euro civarına temin edilebilir.
  - Ancak TPM' in performansı ile bankaların kullandığı kriptografik ek işlemcilerin (IBM 4758 gibi) performansı çok farklıdır.

DRM ve TCPA'e Tepkiler

- Trusted Computing Group ilk kurulduğu zaman adı “Trusted Computing Platform Alliance” idi.
- Platform üyelerinden Microsoft'un sayısal hak yönetimi (DRM) uygulama planları kriptografik beceriler gerektiriyordu.
  - TPM kullanımı bu nedenle Microsoft tarafından “DRM için şart” olarak anlatıldı.
  - DRM karşıtları otomatik olarak TPM ve TCPA karşıtı oldular.
- TCPA iki adım attı.
  - TPM entegrelerinin aktif hale getirilmesi (ve sahip olunması) son kullanıcıya bırakıldı. Fabrikadan çıkan bilgisayardaki TPM aktif değildir.
  - Grup adını TCG olarak değiştirdi.

DRM ve TCPA'e Tepkiler

- Microsoft ve bir çok içerik sağlayıcı şirketin (örneğin Sony) öne sürdüğü DRM modelinde “güvenin kökeni” merkezi bir otoritenin elindedir.
  - Bu otorite “devlet” olmak zorunda değildir. İçerik sağlayıcı şirket yada Microsoft gibi bir şirket olabilir.
  - Güvenin kökenini işleten kişi, belli tür içeriği (istenmeyen şarkı, istenmeyen yazılım) engelleyebilir.
- Bu nedenle kişilerin yada kurumların kendi “güvenin kökeni” sistemlerini kurması gerekir.
  - Ancak bu sistemin kendisine (yazılım bileşenlerine) güvenmek de zor olacaktır.
  - GPL v3 buradaki anlamı ile DRM amaçlı kullanımı yasaklar.

Güvenilir İşletim Sistemi (Trusted OS)

- Peki DRM' i bir kenara koyarsak, Güvenilir Bilişim'in tanımladığı anlamı ile Güvenilir bir İşletim Sistemi nedir ve nasıl çalışır?
- İşletim sistemi yüklenmeden önce BIOS ve benzeri donanımlar TPM kullanılarak doğrulanır.
- Ardından işletim sistemi doğrulanır. Doğrulanmayan işletim sisteminin yüklenmesi (booting) engellenir.
  - İşletim sisteminin güvenli yüklenmesi de (secure booting) önemlidir. İşletim sistemi çekirdeği (kernel) dışında bir çok bileşen de yükleme sırasında bellekte yerini alacaktır.
  - Bu sayede yüklenen işletim sisteminin kendisinin kurduğumuz işletim sistemi olduğundan emin oluruz.
  - Bu mekanizmanın işletim sistemi güncellemesi, yamaların uygulanması, çekirdek derleme gibi etkinlikleri desteklemesi gerekir.

Güvenilir İşletim Sistemi (Trusted OS)

- Güvenli bir biçimde yüklenen işletim sistemi, servisler ve uygulama yazılımları için gerekli bazı alt yapıları sunmalıdır.
  - Her bir uygulamanın süreç uzayı (process space) diğer uygulanmalardan soyutlanmalıdır (isolation). Bu soyutlama özetler veya daha gelişmiş kriptografik tekniklerle desteklenmelidir.
  - Tüm uygulamaların paylaştığı altyapılar, örneğin takas dosyası (swap file) üzerindeki işlemlerin bütünlüğü sağlanmalıdır.
  - Kullanıcı doğrulama (authentication) amaçlı mekanizmalar başta olmak üzere işletim sistemi ve uygulamaların kullanacağı anahtarların güvenliği sağlanmalıdır. Bunun için küçük çaplı bir sertifika otoritesi (local CA) kurulmalıdır.
  - Yazıcı kuyruğu (print spool), eposta kuyruğu (email spool) gibi bileşenlerin gerekli kriptografik desteğe kavuşması gerekir.

Güvenilir İşletim Sistemi (Trusted OS)

- Güvenli bir biçimde yüklenen işletim sistemi, servisler ve uygulama yazılımları için gerekli bazı alt yapıları sunmalıdır.
  - Hem sistem hem de kullanıcı düzeyinde güvenilir veri saklama (trusted storage) ve güvenilir kurtarma (trusted recovery) sağlanmalıdır.
  - Grafik kullanıcı arabirimi olan uygulamaların hareketlerinin kaydedilmesinin isteğe bağlı olarak engellenmesi gerekebilir. Bunun için GUI bileşenleri arası haberleşmenin şifreli olması seçeneği gerekir.
  - Sayısal imza uygulamalarında imzalanan belgenin ekrandaki görüntüsünün aslında imzalanan belge olup olmadığının doğrulanması (what you see is what you sign) gerekir. Bu da yine GUI seviyesinde güncellemeler gerektirecektir.

Microsoft Vista

- Microsoft'un yeni güvenlik modeli işletim sisteminin kademeli olarak Güvenilir İşletim Sistemi durumu kazanmasını öngörür.
  - Bu çok iyi bir gelişmedir.
- MS Longhorn' un gecikmesi ve sonra Vista olarak yeniden adlandırılması da bu konudaki iyileştirmeler ve geliştirmelerin sonucudur.
  - Microsoft Windows'un geleneksel mimarisi bu tür değişikliklere pek açık değildir. Bu nedenle gelişmeler ciddi anlamda zaman almaktadır.
  - Ancak Vista' dan itibaren gelecek olan Windows işletim sistemlerinin güvenlik becerilerinin ciddi oranda artacağını kabul etmeliyiz.

Trusted Linux

- Linux tek bir firmanın geliştirdiği bir ürün değildir. Trusted Linux diye adlandıracağımız bir işletim sistemi çok sayıda farklı kaynaktan gelen bileşenlerin gelişmesini gerektirecektir.
  - Çekirdek ve modülleri
  - Temel ağ servisleri
  - X ve X üzerindeki pencere yöneticileri (KDE, Gnome, vs.)
  - Bir çok yaygın uygulama
- Bu nedenle Trusted Linux çalışmaları dağınıktır. Debian, Gentoo ve Suse ekiplerinde bu çalışmalar olduğu bilinmektedir.
- Ancak Linux'un mimarisi gerekli güncellemelere çok açık bir yapıdadır.
  - Dağıtık geliştirme Linux'un çok daha modüler olmasını, gerekli soyutlamaların zaten hazır gelmesini sağlamıştır.

Trusted Linux

- Trusted Linux'a ulaşmak için gerekli ilk adım çoktan atılmıştır.
  - Çekirdeğin sanallaştırılması (kernel virtualization) adı verilen bir teknik ile işletim sisteminin bir anlamda kendi çekirdeğinden bağımsız hale gelmesi sağlanmıştır.
  - Bu sayede aynı bilgisayarda (işlemcide) aynı anda birden fazla ve hatta farklı işletim sistemi çekirdeği çalışabilir.
  - Bunun için XEN ve L4 adında iki yaygın yaklaşım bulunmaktadır. XEN yaklaşımı Fedora Core 4 ve Suse 10.0'da denemek üzere hazır gelmektedir.
  - Bu tür bir teknoloji şu anda herhangi bir Windows işletim sisteminde yoktur.
- Bundan sonra gerekli çekirdek güncellemelerinin yapılması ile temel atılmış olacaktır.

Open Trusted Computing

- Güvenilir Linux alanındaki önemli çalışmalardan birisi de Avrupa Birliği 6. Çerçeve Programı kapsamında desteklenen Open Trusted Computing projesidir.
  - Proje 23 Avrupalı ortağın oluşturduğu bir konsorsiyum tarafından yürütülecektir ve 1 Kasım 2005 tarihinde başlamıştır. Proje 6ÇP kapsamında verilen en büyük desteklerden birisini almıştır.
  - Proje hedefi Güvenilir Linux için gereken çekirdek düzenlemelerinden kavram ispatı (proof-of-concept) güvenlik uygulamalarına kadar geniş bir yelpazede kod üretmek, bu kodların kullanımını yaygınlaştırmak ve ayrıca toplumdaki yanlış inanışları düzeltmektir.
  - Türkiye'den Portakal Teknoloji özel sektör, TÜBİTAK/UEKAE ise araştırma merkezi statüsünde katılmaktadır.

Open Trusted Computing

- Projenin ilk aşaması yoğun bir spesifikasyon yazımı sürecidir.
- Projenin kalabalık doğası ve yapılacak işin kapsamının genişliği aynı işin birden fazla kez yapılmasına neden olabilir.
  - Bunun önüne geçmek için gereken ortak altyapıların ve bunların nasıl kullanılacağının çok iyi saptanması gerekmektedir.
  - Bu spesifikasyon çalışması 2006 yılı içerisinde sona erecektir.
  - Ancak bazı alt başlıklarda geliştirme çalışmaları da devam etmektedir.
- Projenin çıktıları GPL olacaktır. GPL v3'deki DRM ile ilgili ifadeler nedeni ile GPL sürümü konusu henüz netlik kazanmamıştır.
  - Proje çıktılarının kamuya ait olması AB'ye verilen bir taahhüttür. Bu nedenle patentler ve benzeri sınırlandırmalar olmayacaktır.

The Open-TC project is partly sponsored by the EC.

If you need further information, please visit our website www.opentc.

Technikon Forschungs- und Planungsgesellschaft mbH
Richard-Wagner-Strasse 7, 9500 Villach, AUSTRIA
Tel. +43 4242 23355 – 0
Fax. +43 4242 23355 – 77
Email coordination@opentc.net