



Trusted Computing ve Linux

Bora Güngören
Portakal Teknoloji
bora@portakalteknoloji.com
Bilgi Üniversitesi
24.02.2006

- Güven Kavramı
- Güvenilir Bilişim (Trusted Computing)
- Güvenilir İşletim Sistemi (Trusted OS)
- Politikalar (Enforced Policies)
- Doğrudan Anonim Doğrulama (Direct Anonymous Attestation)
- Örnek Uygulamalar (Examples)
- Microsoft NGSCB
- Trusted Linux
- Open Trusted Computing

- 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 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)
- Bu dört bileşenin sağlanması için çeşitli örnekleri yeniden gözden geçirelim.
 - Kimlik kartları, çek defterleri, kredi kartları, nakit para, noter kayıtları, ticari sicil, adli sicil, tapu kaydı, vs.
 - Hiç biri salt bilişim teknolojilerine özel uygulamalar değil.

- Bilişim teknolojileri ve getirdikleri uygulamalar günümüzdeki hali ile son derece kuvvetli güven ilişkilerinin zaten var olduğuna dair varsayımlara dayanır.
- Eposta sistemini ele alalım.
 - Bugün aldığımız epostaların kaynağından emin olmamız neredeyse mümkün değildir.
 - Birisine yolladığımız epostanın karşı tarafa ulaştığını doğrulamak için kullandığımız mekanizmaya güvenemeyiz.
 - Eposta içeriğinin doğruluğundan emin olamayız.
- Bunların basit çözümleri bugün de vardır ancak bu çözümleri aldatmak mümkündür.
 - Esas mesele, çözümün aldatıldığından emin olamayız.



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.
 - Varsayılan güven (assumed trust) yerine doğrulanabilir güven (verifiable trust) geçer.



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 (Transmeta Crusoe, Intel LaGrande, AMD Pacifica, ARM?, Power?, Sparc?)
 - TPM ana karttaki başka bir entegrenin içine gömülebilir (Broadcom Gigabit Ethernet)
 - TPM özellikle güvenilir olmak isteyen bir donanımda ayrıca bulunabilir. (Seagate'in prototip diskleri, bazı USB bellek projeleri)



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.
 - Büyük ölçekli kripto performansı için bu ek işlemcilere ihtiyaç devam etmektedir.



Güvenilir İşletim Sistemi (Trusted OS)

- 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 uygulamalardan 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.

- Güvenilir Bilişim'in getirdiği en önemli yeniliklerden birisi de verinin kendisi ile ne yapılabileceği hakkındaki politikaları yanında taşıyabilmesidir.
- Politika bilgisi tıpkı gerçek bilgi gibi kriptografik tekniklerle korunur.
 - Koruma mekanizmasının güvенеceği bir kökene ihtiyacı olur. Bu görevi TPM üstlenir. Her bir politikanın kendisi üzerinde değişiklik yapılmadığını TPM'i kullanarak doğrularız.
 - Bu işi yapmanın bir yolu, normalde kriptolu olarak saklanan politikayı TPM'in içinde açmaktır.
- Böylece veriye erişim nereden yapılırsa yapılsın, güvenilir platformlarda bu politikaların değişmeden kalacağı kesindir.
 - Dolayısı ile politikalara “enforced policy” adı verilir.

- Elbette ki her politika bu kadar katı olmak zorunda değildir. Bazı politikalar dinamik olarak değiştirilebilecek biçimde tasarlanabilir.
- Bu biçimde politika kullanımı tamamen spesifik uygulamaların tasarımına bağlıdır.
 - Bir ofis yazılımı kendi belge biçimine politikalar ekleyebilir.
 - Bu politikaların varsayılan davranışı sanki politikalar yokmuş gibi olabilir.
 - Kullanıcı belgeye kendisi (yada sistem yöneticisi) tarafından tanımlanan politikaları ekler.
 - Ayrıca belge bir dosya olacağı için işletim sisteminin tüm dosyalara ekleyeceği varsayılan politikalar da geçerli olur.
- İşletim sistemi tarafından dayatılacak olan varsayılan politikalar yine önemli bir tartışma alanıdır.



Doğrudan Anonim Doğrulama (DAA)

- Güvenilir Bilişim'in en çok tartışılan kısımlarından birisi TPM'lerin kimliklerinin saptanmasıdır.
 - TPM üreticisinin de katkısı olsa dahi gerektiğinde bu bilginin saklanması gerekir.
- Doğrudan Anonim Doğrulama (Direct Anonymous Attestation – DAA) bir kriptografik varlığın (bizim için TPM yada TPM kullanıcısı) kimliğini açığa vurmaksızın bazı yetkilerinin olup olmadığını doğrulatabilmesine olanak verir.
 - Böylece kim olduğumuzu açıklamadan bir çok işlemi yapabiliriz.
- DAA ayrıca TPM'i olan bir bilgisayarın ikinci el olarak satılması durumunda, yeni sahibinin eski sahibinin yerine geçeceği saldırıları ve kimlik açığa çıkarma çabalarını da engelleyecek biçimde tasarlanmıştır.

- Eposta sistemine geri dönelim.
 - Epostalarınızı sadece kimliğini onayladığınız SMTP sunucuları aracılığı ile aktarılmasını sağlayabiliriz.
 - Epostalarınızın içeriğine yönelik koruma mekanizmalarına artık güvenebiliriz.
 - Yolladığınız epostanın alıcısının neler yapabileceği üzerine bir politika belirleyebilirsiniz. Karşı tarafta bu politika uygulanacaktır (enforced policy)
 - Sadece okusun (read only)
 - Okusun ve yanıtlasın (read and reply)
 - Yönlendirebilsin (can forward)
 - Sadece belli bir alan adındaki adreslere yönlendirebilsin (limited forward)
 - Anonim kalacağınız garantilenmiş (guaranteed anonymity) mesajlar yollayabilirsiniz.

- Tipik bir edevlet uygulaması olarak emniyet bilgi sistemini (police information system) ele alalım.
 - Şu anda herhangi bir polis memuru, herhangi bir yerden bağlanıp bir çok bilgiye ulaşabilir.
 - Yine politikaların (enforced policy) eklenmesi ile kişilere ait bilgilere sadece o kişilerle ilgili bir uygulama eylemi başlatan bir memurun erişmesi sağlanabilir.
 - Örneğin sizinle ilgili bir tutanak tutuluyorsa, o tutanağın tutulması için uygun görülen bir terminalden bağlanılıyorsa ve o anda sisteme bağlanan memur görev çizelgesine göre o işi yapmaya yetkili kılınmışsa, bilginize ulaşılır.
 - Artık keyfi biçimde sizin bilgilerinize ulaşmak mümkün olmaz.
 - Böylece kişisel bilginin korunması daha etkin biçimde sağlanır.
 - Devletin kişisel bilgileri güvenli biçimde saklama (personal privacy) yükümlülüğü sağlanır.

- Bir iş akışı (workflow) uygulaması, tipik olarak kişilerin belli başlı dosya türlerinden dosyalar ile çalışmasını sağlar.
 - Bir müşterinin siparişi, bir iş emrini (work order) tetikler ve bu emirle ilgili bir metin belgesi yaratılabilir.
 - Kullanıcılar bu belgeyi, bir sürümlendirme mekanizması eşliğinde, değiştirirler ve belge üzerinde kendi yetkileri çerçevesinde değişiklikler yaparlar.
 - Acaba bu belge üzerinde izinsiz değişiklikler yapılabilir mi?
 - Belge sistem dışarısına sızdırılabilir mi?
 - Eğer belgenin içinde uygun politikalar tanımlanmışsa bunlar yapılamaz.

- Bir veri tabanı (database) uygulaması için tek tek dosyalar değil de tablolar (tables) ve benzeri özel yapılar vardır.
 - Politikaların bu yapılar için tanımlandığını varsayalım.
 - Her bir SQL sorgusunun erişebileceği tablolar ve kayıtlara dayanan bir yetki modeli oluşacaktır. Bu model içerisinde yeterli yetkileri olmayan kullanıcılar SQL komutlarını çalıştırsa bile pratikte bir sonuç elde edemez.
 - Böylece “SQL Injection” adı verilen türdeki saldırıların önemi azalır. Sadece ilgili yetkiye sahip ekranlar risk oluşturur.



Örnek Uygulamalar (Examples)

- Bütün bu uygulamalarda kullanılan kriptografik teknikler uzun süredir kullanımdadır.
- Bu tekniklerin bir işletim sisteminde sistematik olarak uygulanması ve bu uygulamanın TPM türü bir donanım ile desteklenmesi fikri de yeni değildir. Askeri yazılımlar ve işletim sistemleri bunları yıllardır uygulamaktadır.
 - Yeni olan bu fikirlerin siivil ve ticari olarak nitelendirdiğimiz yazılımlarda uygulanmasıdır.
 - Elbette uygulama alanındaki farklardan dolayı yepyeni ihtiyaçların (kişisel gizlilik ve anonim kalma hakkı gibi) tanımlanması ve teknolojinin bu haklara saygı gösterecek uygulamalar sağlaması gerekmektedir.

- Microsoft'un yeni güvenlik modeli işletim sisteminin kademeli olarak Güvenilir İşletim Sistemi durumu kazanmasını öngörür.
- Bu mekanizmalara topluca “Next Generation Secure Computing Base” adı verilmektedir.
 - Bu bir çok kişi için çok iyi bir gelişmedir.
 - Ancak sistemin açık olmaması şüpheleri de otomatik olarak çekmektedir.
- NGSCB'in gerçekleşmesi için sadece Microsoft'un değil, başka bir çok donanım ve yazılım üreticisinin de yapacak çok şeyi vardır.

- 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. Vista'da mimari değişecektir. Bu nedenle gelişmeler ciddi anlamda zaman almaktadır.
 - Böylece Vista' dan itibaren gelecek olan Windows işletim sistemlerinin güvenlik becerilerinin ciddi oranda artacağını kabul etmeliyiz.

- 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.
 - Örneğin Linux içerisinde bir çok bileşen zaten soketlerle haberleşmektedir. Bu haberleşmenin güvenlik mekanizmalarını kullanacak biçimde yeniden düzenlenmesi mümkündür.
 - Uygulamaların kendi anahtarları olduğu anda uygulamalar arası (inter-application) PKI kullanılabilir.
 - Her kurulan uygulamaya yeni bir anahtar verilmesi için TPM, bu anahtarların saklanması için bir yerel sertifika otoritesi (local CA) kullanılabilir.
 - Sadece bir kaç yaygın kabuğun (shell) yeniden yazılması otomatik olarak bütün betik uygulamalarına (sed, awk, perl, python) yarar.

- 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.
 - Kurulum sırasında seçerek XEN'i kullanmaya başlayabilirsiniz.
 - Hem XEN hem de L4 açık kaynak kodludur.
 - Bu tür bir teknoloji şu anda herhangi bir Windows işletim sisteminde yoktur.

- Güvenilir bilişimin Linux üzerinde gerçekleşmesi, teknik rekabet nedeni ile zorunludur.
 - Kurumlar güvenilir bir Windows ile uyumsuz olacak güvenilir olmayan Linux'ları kullanmayacaktır.
 - Güvenilir olmayan Linux'ların güvenlik becerilerini ayakta tutmak giderek zorlaşacaktır.
- Güvenilir bilişimin Linux üzerinde gerçekleşmesi, politik bir zorunluluktur.
 - Güvenilir bilişimin kapalı kaynak kodla gerçekleşmesi, her zaman gördüğümüz “büyük ağabey” korkularının daha da derinleşmesine yol açacaktır.
 - Özellikle işletim sisteminin bu teknolojiyi nasıl kullandığının net biçimde bilinmesi gerekir.

- Bir Güvenilir Linux (Trusted Linux) gerçeklemesi için gereken bir çok şey hazır olmakla birlikte GPL v3 açık biçimde DRM amaçlı uygulamaların GPL olmasını engellemektedir.
 - Yasal zorlamalar eninde sonunda işletim sistemlerinin DRM konusunda becerileri olmasını isteyecektir.
 - O zaman ileride bu tür becerileri olan işletim sistemlerinin (herhangi bir Linux dağıtımı) GPL v3 olmasında sorun çıkabilir.
 - Bu konu aslında Linux Kernel eposta listelerinde tartışılmıştır.
 - Stallman bunu açık biçimde vurgulamış ve ileride Linux çekirdeğinin GPL olarak nitelenmesine engel olabileceğini söylemiştir.
 - Torvalds ise, “önemli olanın tüketicilerin gereksinimleri olduğu” vurgusunu yapmıştır. Torvalds'a göre gerekirse “patentle korunan kod bile” bu amaçla çekirdeğe eklenmelidir.
- Tartışma aslında DRM tartışmasıdır, TC için içinde sadece bir teknoloji olarak yer almaktadır.



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 kullanılacağına 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.

- Portakal Teknoloji'nin OPEN_TC içerisinde yaptığı bir uygulama TC destekli bir Kriptolu Dosya Servisi (Encrypted File Service) yazılmasıdır.
 - Servisin geleneksel kriptolu saklama araçlarından öncelikli farkı TPM ile gelen bütün özellikleri net biçimde kullanması olacaktır.
 - Özellikle politikalar konusunda kullanıcının özgürlüğünü (freedom of the user) temel alacak ancak kurumsal uygulamaların gereksinimlerini de gözardı etmeyecek bir denge kurulması amaçlanmaktadır.
 - Bu uygulamanın bir yan ürünü de diğer uygulamaların kullanacakları bir C/C++ API'sidir. Bu API ile uygulama geliştiriciler kendi uygulamalarında EFS becerilerine sahip olabilir.



Open_TC EC Contract No: IST-027635

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

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

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

- The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.