



Güvenilir İşletim Sistemi Mimarileri

Volkan Erol

TÜBİTAK UEKAE

Bora Güngören

Portakal Teknoloji

LKD Linux ve Özgür Yazılım Şenliği, ODTÜ – Ankara

12.05.2006

- Genel Güvenlik Problemleri
- Güvenilir Bilişim Durum Tespiti
- Güvenilir İşletim Sistemi – Temel Hizmetler
- Güvenilir İşletim Sistemi – İleri Hizmetler
- Open Trusted Computing Projesi
- Sorular



Genel Güvenlik Problemleri

- Salt yazılım tabanlı güvenlik çözümlerine ne kadar güvenebiliyoruz? Bir türlü çözemediğimiz sorunları düşünün:
 - Çeşitli ve sürekli artan saldırılar
 - Virüs solucan gibi sorunlar
- Yeni bir yaklaşım sistemin güvenliğini donanım ile sağlamaktır.
 - Sistemin güvenliği donanım seviyesindeki bir köken ile kontrol edilir.
 - Güvenlik sistemi istenilen konfigürasyonda tasarlanır
 - Bu yaklaşımın örneklerinden birisi Güvenilir Bilişim (Trusted Computing) olarak adlandırılıyor.

- Gerçek hayatta kime güveniriz? Peki yazılımlarda?
 - Kullandığımız yazılımlara güvenmeli miyiz?
 - İşletim sistemine güvenmeli miyiz?
 - Aygıt sürücülerine güvenmeli miyiz?
 - Donanımların içindeki gömülü yazılımlara güvenmeli miyiz?
- Kime güvенеceğimizi bilemezsek, hiç bir güvenlik çözümünün çalıştığından emin olamayız.
 - Güvenebileceğimiz güvenlik çözümlerini kurgulamak için güvenebileceğimiz en az bir adet bileşen olmalıdır.
 - Klasik yöntemler (güvenlik duvarı + anti virüs kapısı örneği) burada yetersiz kalır.
 - Güvenilir bilişim burada devreye girer.

- Sayısal imza ve açık anahtar altyapısı (RSA şifrelemesi) aslında bizim için gerekli altyapıyı genel olarak kurgular.
 - Her türlü sistemi sayısal imzalar ve açık anahtar altyapısı ile güvenilir kılabiliriz.
 - Ancak anahtar altyapısının kendisinin güvenilir olması gerekir.
- Trusted Platform Module (TPM) altyapısının güvenilir olması için gereken asgari bileşendir.
 - BIOS'dan başlayarak en üst katmana kadar tüm doğrulama ve güvenilirlik denetimleri
 - Bütünlük denetimleri
 - İstenirse, sertifikalı donanım ve yazılım kısıtlamaları
 - Her adımda istenen konfigürasyonda çalışma denetimi ve garantisi

- Bugün 20-30 milyon arasındaki kişisel bilgisayarda TPM bulunmaktadır. Kişisel haklara saygı için bu bileşenler kapalı gelmektedir. Aktif hale gelmeleri son kullanıcıya (yada kurum bilgi işlemine) bırakılmıştır.
 - Bunun sonucu olarak TPM'in ne olduğunu ve kullanım alanlarını bilen kişilerde bile TPM'ler kapalı kalmaya devam eder.
 - Ancak aynı kişilerde TPM'i ilkel seviyede de olsa kullanmaya hazır yazılımlar bulunmaktadır. Yani TPM'lerin kapalı olması kısıtlı olsa da yararlanılmasını engellemektedir.
 - Bireylerin ve kurumların TPM'in varlığı ve nasıl kullanılabileceği konusunda eğitilmesi gerekmektedir.

- TPM'lerin içindeki anahtar deposu becerisi kullanıcılardan çok kurum bilgi işlemlerinin ilgisini çekmektedir.
 - Özellikle diz üstü bilgisayarların çalınması durumunda bilgisayarda bulunan anahtarların ve sayısal imza bileşenlerinin daha sonra kötü amaçlı kullanımı önemli bir risktir.
 - TPM'in bu anahtarlar için depo görevi görmesi, çalınan bir dizüstü bilgisayarın saldırı amaçlı kullanımını neredeyse imkansız hale getirir.
- TPM'in DRM için kullanımı örneği yoktur. Tartışılan DRM ürünleri (örneğin Sony) bu becerileri kullanmaz.
 - Yaygın kanının aslında gerçekte ilgisi olmadığı görülmektedir.
 - Microsoft X-Box 2'deki DRM modülünün standart uyumlu olmayan bir TPM ile sağlandığına dikkat çekmekte de yarar vardır.

- Güvenilir Bilişim için önümüzdeki dönemde en yaygın uygulama potansiyeli şu alanlarda görülmektedir.
 - Virüsler, solucanlar ve daha sonra saldırı amaçlı kullanılacak benzeri açıkların engellenmesi.
 - Çok sayıda bilgisayar olan ağlarda ve dizüstü bilgisayarlarda çalınan bilgisayarların kullanılmasını engellemek ve diskleri bloklamak (örneğin Seagate'in bu alanda prototip bir diski vardır).
 - Kablosuz ağ ve VPN'lere erişimin daha güvenli kılınması için sadece kimliği doğrulanan bilgisayarların bağlanmasına izin verilmesi.
 - İstemci sunucu uygulamalarında istemcinin durumunun denetlenmesi.
 - Evden çalışan kişilerin kendi kişisel bilgisayarları ile iş ağlarına bağlanmasının yönetilmesi.

- Sunucuların söz konusu olduğu her durumda Güvenilir Bilişim önemli katkılar sunacaktır.
 - Sunucu üzerindeki çok sayıda işletim sisteminde çalışan sunucuların (örneğin Linux/Apache ve Windows/IIS) istemciler için saydamlaşması sağlanabilir. Bu ağların yönetimini kolaylaştırır.
 - Uzaktan destek tekniklerinin güvenliği artar.
- Ancak ne yazık ki piyasada TPM sahibi sunucu donanımı bulmak güçtür.
 - IBM'in sadece bir modeli (x3850 – 3U kasa – asgari 7-8 bin dolar) bu donanıma sahiptir.
 - Diğer OEM'lerde bu tür bir model yoktur.
 - Intel'in sunucu odaklı ve TPM sahibi anakartları bin dolar seviyesinde fiyatlanmaktadır.

- Güvenliğin kritik olduğu uygulamalarda klasik çözüm uygulamaların fiziksel olarak ayrılmasıdır.
 - İki bilgisayarım var. Birisi oyun oynamak için; ötekinde sadece İnternet bankacılığı yapıyorum.
- Güvenilir bilişim ile bu senaryo değişir.
 - Tek bilgisayarım var. Aynı anda iki sanal makinada iki farklı işletim sistemi çalışıyor. Birisinde oyun oynuyorum; ötekisinden bankaya giriyorum.

- Mobil platformda TPM uygulamaları da olasıdır.
 - SIMLOCK saldırıları, başkasının hattını kullanma gibi uygulamalar tarihe karışacaktır.
- Ancak TPM'lerin 2-3 Euro'luk maliyetleri henüz mobil piyasa için yüksektir.
 - PC kullanıcıları sadece işlemcilerine 100 Euro ve üzeri fiyatlar ödemeye alışıktır.
 - Ancak bir cep telefonu zaten 100 Euro'nun altında satılmaktadır.
- Ayrıca TPM'lerin güç karakteristikleri de mobil piyasanın gereksinimleri için fazla talepkardır
 - Güvenilir ama şarjı hemen biten bir cep telefonu?

- Görüldüğü gibi Güvenilir Bilişim çok ciddi bir potansiyele sahiptir.
 - Kısa sürede dünyadaki bilgisayarların makul bir yüzdesinin TPM ile donanmış olduğunu düşünürsek orta dönemde neredeyse tüm bilgisayarların bu donanıma sahip olacağından emin olabiliriz.
 - Ancak insanların ve kurumların, özellikle de yazılım şirketlerinin bu konuda doğru bilgilendirilmesi gereklidir.
 - Medyada TPM = DRM türü bir yanlış anlama yaygındır. Bu yanlış anlamamanın önüne geçmek için teknik gerçeklere dayanan bir sunum sağlanmalıdır.
 - Kişisel hakların korunması için 1.2 sürümüne eklenen DAA (doğrudan anonim doğrulama) özelliğini kullanan uygulamalar geliştirilmelidir.

- Temel prensip iki ayrı teknolojiyi harmanlamaktır.
 - İşletim sistemi sanallaştırması (virtualization) sisteme yüklenen işletim sisteminin bir başka bileşen tarafından doğrulanmasını sağlar.
 - Bu bileşene hypervisor adını vermekteyiz.
 - XEN ve L4 olarak iki açık kaynak kodlu hypervisor bulunmaktadır.
 - Suse ve Fedora'da standart bir kurulum seçeneği olarak Xen'i seçebilirsiniz.
 - TPM'e erişim sağlayan Güvenilir Yazılım Yığını (Trusted Software Stack – TSS) ise genel kriptografik becerileri sunacaktır.
 - TSS için Windows ve Linux'da zaten hazır kodlar ve aygıt sürücüleri vardır.
 - Trousers açık kaynak kodlu TSS referans alınmaktadır.

- Hypervisor ne yapacaktır?
 - Her işletim sistemi bir sanal makinada çalışacaktır.
 - Hypervisor bu durumda işletim sistemlerinin donanıma erişmesi için arabirim görevi görecek. Bu da iki işletim sisteminin aynı donanıma erişmesinde kilitler gibi mekanizmalar sağlar.
 - Örneğin, birinci işletim sisteminin ağ trafiğini ikinci işletim sistemi izleyemez.
- Bu yapıda bir sanal makinede başarılı olan bir saldırı diğer sanal makinelere bulaşamaz, zarar veremez ve hizmeti kesintiye uğratamaz.
 - Peki sunucu uygulamalarını doğrudan hypervisor üzerinden çalıştırsak?

- Hypervisor'ün yüklediği işletim sisteminin durumu (state) denetlenebilir.
 - Durumunu beğenmediğimiz bir işletim sistemini yüklemeyi durdurabiliriz.
 - Ancak çekirdek güncellemesi, yama kurulması gibi durumlarda yeniden başlatılan sistemin yüklenebilmesi için “önceki durum” ve “son durum” olarak iki durum saklanmalıdır.
 - Durumun saptanması için kritik dizinlerin ve dosyaların oluşturduğu bir kümenin (örneğin /boot disk bölümündeki çekirdek imajı) MD5 toplamının alınması yeterli olacaktır.
- Temel bir hypervisor desteği için işletim sisteminin sanallaştırmadan haberinin olması yeterlidir.
 - Şu anda XEN kullanan Linux dağıtımları bunu kullanmaktadır.

- Güvенеbileceğimiz donanımlar, TPM/TSS ve işletim sisteminden oluşan bütüne Güvenilir Bilişim alt yapısı diyebiliriz.
 - Yazılımlar bu altyapıyı varsayacak biçimde yazılabilir.
 - Bu durumda bazı güvenlik teknikleri ya kolay uygulanacak ya da gereksiz olacaktır.
- Peki güvenilir altyapı uygulamalara ne sunar?
 - Uygulamaların süreçleri izole edilir.
 - Süreçler yüklenmeden önce doğrulanır.
 - Güvenilir bir şifreleme ile diskte veri saklanabilir.
 - RSA, vb açık anahtar uygulamaları yaygınlaşır.

- Daha gelişmiş bir güvenilir bilişim altyapısı hypervisor kullanımını daha da ileri noktalara götürür.
 - Artık işletim sistemleri hypervisor üzerinde çalıştıklarının farkında değildir.
 - Yani herhangi bir işletim sistemini hypervisor üzerine kurabilirsiniz.
 - Donanım aygıt sürücüleri de hypervisor tarafından kullanıldıklarından habersiz çalışır.
 - Yani herhangi bir işletim sisteminin aygıt sürücüsü, her işletim sistemi için geçerli olur.



Open Trusted Computing Projesi

- Güvenilir Bilişim 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 TÜBİTAK/UEKAE araştırma merkezi, Portakal Teknoloji özel sektör statüsünde katılmaktadır.



Open Trusted Computing Projesi

- 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.



Open Trusted Computing Projesi

- TÜBİTAK UEKAE kurum içi mesaj deęiřimi (message exchange) için bir altyapıyı Güvenilir Biliřim teknolojisini kullanan bir grup sunucu ile gerçekleřtirecektir.
- Portakal Teknoloji'nin ise OPEN_TC ięerisinde Güvenilir Biliřim destekli bir Kriptolu Dosya Servisi (Encrypted File Service) uygulaması geliřtirecektir.



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

If you need further information, please visit our website www.opentc.net or contact the coordinator:

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.