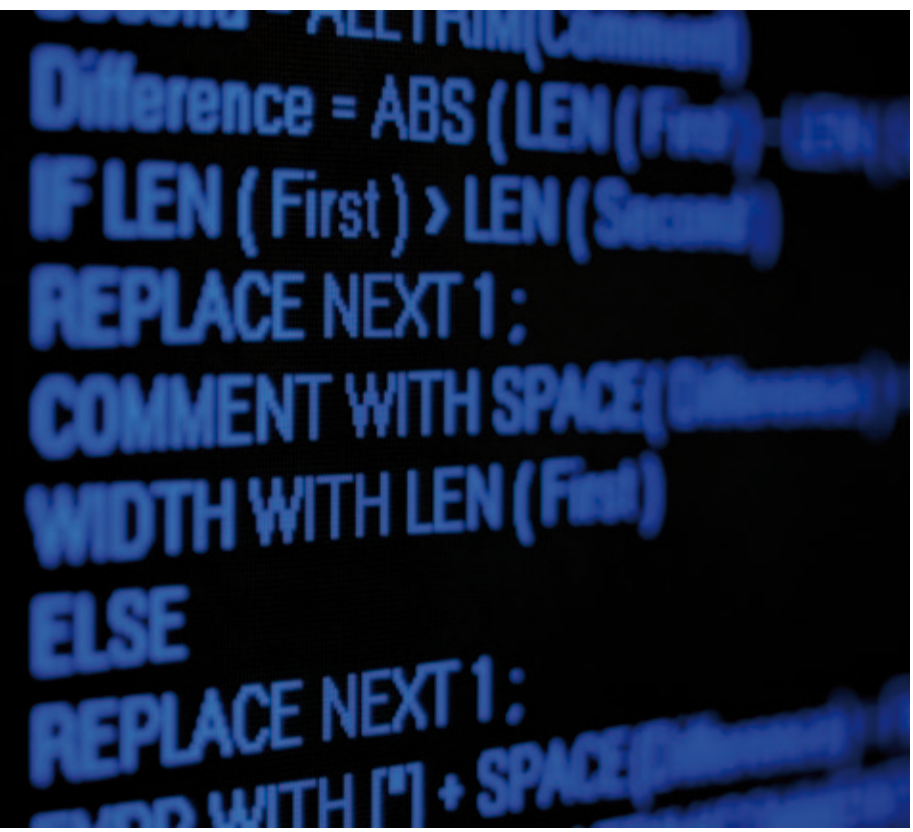
Erkay Savaş

Güvenilir Hesaplama

Günümüzde bilgisayarları kullanarak gerçekleştirdiğimiz işlemlerin hem sayısı ve çeşidi artıyor hem de bu işlemlerin ciddiyeti. Genelde bilgisayarlarla gerçekleştirdiğimiz işlemlere daha çok güvenme eğiliminde olduğumuz gözlenen bir olgu. Ancak bilgisayarlarla yaptığımız işlemlerin sonuçlarına gerçekten ne kadar güvenebiliriz? Hesaplama yetenekleri ve çeşitliliği giderek artarken, yapıları bir o kadar karmaşıklaşan bilgisayarlar bize ne türlü güvenceler verebilir? Hesaplamada güvenilirlik, bilgisayar hızını ve kapasitesini artırmak türünden *yalnızca* teknolojik olarak ele alınabilecek bir konu değil. Kullanıcıların kabul edeceği, hukuki bağlayıcılığı olan ve teknolojik olarak kolayca gerçekleştirilebilecek çözümlere gereksinim olduğu ortada.



Günümüzde hızla ilerleyen teknoloji konusunda ülkemizde bir farkındalık yaratmak için ele alınması gereken öncelikli konulardan biri, kabul edilebilir ve daha önce kullanılanla uyumlu bir terminoloji geliştirilmesidir. *Güvenilir hesaplama*, bu konuda dikkatli olunmazsa sorunlar yaratabilecek, kolayca yanlış anlamalara yol açabilecek türden bir konu. Güvenilir hesaplama, İngilizce'de kullanılan "*trusted computing*" kavramını karşılamak için kullanılan bir terim. Güvenli hesaplama (İngilizce "*secure computing*") ile yakından ilintili olmasına rağmen ayrı bağlamlarda ele alınması gereken bir alan.

Güvenilir Bir Bilgisayardan Beklenenler

En basit tanımına baktığımız zaman, güvenilir hesaplama bir bilgisayarın daha önceden belirlenmiş spesifikasyonlar çerçevesinde davranması ve bunun donanım ve yazılım yardımıyla gerçeklenmesidir. Daha yalın bir ifade ile belirtmek gerekirse, kullandığımız diğer tüm cihazlarda olduğu gibi, bilgisayarın da komutlarımıza uymasını ve bu-

nu bize söylenen spesifikasyonlara uygun bir şekilde gerçekleştirmesini bekleriz. Bir analoji kurmak istersek, otomobilimizin fren sistemini düşünebiliriz. Fren pedalına bastığımızda otomobilimizin, hızına ve fren sisteminin bakım koşullarına bağlı olarak, belirli bir mesafede durmasını bekleriz. Durup durmadığını sınamak da çok kolaydır, ancak özen ve dikkat gerektirir. Bu beklentimiz, üretici tarafından ilan edilen spesifikasyonlar, üreticinin tabi olduğu üretim şartnameleri ve bağımsız üçüncü parti testleri sonucunda oluşmuştur. Dolayısıyla, otomobilimizin fren sisteminin belirli bir şekilde çalışması konusunda çeşitli taraflar tarafından oluşturulmuş bir güven söz konusudur ve bu nedenle normal koşullarda otomobilin frene bastığımızda duracağına olan inancımızın yüksek olması beklenir.

Aynı şekilde, bilgisiyarımızın da bize söylendiği gibi davranmasını bekleriz. Arkadaşımıza bir e-posta gönderdiğimizde, beklentimiz bilgisayarımızın bu mesajı değiştirmeden hedeflenen kişiye göndermesidir. Bilgisayarımızdaki kişisel ve başkalarının görmesi sakıncalı olan gizli bilgilerin e-postamızla birlikte gönderilmediğinden nasıl emin olabiliriz? Ya da banka hesabımızda yaptığımızı sandığımız işlemlerin, yapıldığını düşündüğümüz şekilde gerçekleştirildiğinden nasıl emin olabiliriz? İnternete bağlandığımızda, istemimiz dışında ağ bağlantıları oluşmasını nasıl önleyebiliriz?

Güvenilirlik konusunu, otomobil gibi genelde tek amaçlı cihazlarda çözümlemek çok daha kolaydır. Otomobilin insanları bir yerden bir yere götürmek gibi tek bir amacı vardır (bazen insanlar otomobili değişik amaçlar için de kullanabilir -içinde uyumaktan tutun çocukların eski otomobilleri oyun alanı olarak kullanmasına kadar- ancak bu genel kuralımızı değiştirmez). Bilgisayar bu anlamda tek amaçlı bir alet değildir. Kimilerimizin bilgisayarı kullanmadaki tek amacı sadece oyun oynamak ya da film seyretmek olsa da, bilgisayar çok amaçlı olarak kullanılması hedeflenerek tasarlanmış bir cihazdır. Bilgisayarla oyun oynayıp film seyredebildiğimiz gibi, e-posta gönderir, bankaya çevrimiçi bağlanır, para transferi yapabiliriz. Bunun dışında, bilgisayarlar iş dünyasının ve bilimsel araştırmaların da ayrılmaz bir parçası oldu. Kısaca bilgisayarlarla gerçekleştirebileceklerimizin sınırını şu an için kestirmek çok zor. Ancak aynı şekilde, kötü niyetli kişilerin bilgisayarlarımızın güvenlik açıklarından yararlanarak neden olabilecekleri zararların boyutunu tahmin etmek de neredeyse imkânsız.

Kötü niyetli kişiler, bilgisayardaki kişisel bilgilerimizi ele geçirebilir, banka işlemlerimizi kontrol edebilir, kişisel bilgisayarımızı ele geçirip başka noktalara saldırmak için kullanabilir. Bu örnekler kolaylıkla çoğaltılabilir. Ancak, güvenilir hesaplama bağlamında asıl ciddi ve vahim durum, bütün bunlar olurken kullanıcının ya da bilgisayar sahibinin bütün bunlardan haberinin olmamasıdır. Çünkü kullanıcı güvendiği bir üreticinin bilgisayarını kullanmaktadır ve bilgisayarının üzerindeki tüm yazılımlar yine güvenilir yazılım firmaları tarafından geliştirilmiştir, kullanıcı kendisine söylenen tüm güvenlik önlemlerini almıştır. Buna rağmen işler ters gidebilir.

Kullanıcının banka hesabına çevrimiçi ulaşıp para transferi yapmak istediğini düşünelim. Kullanıcı internet üzerinden güvenli ve şifreli olarak işlem yapıyor. Yine de kendi bilgisayarında zararlı bir programın çalışıp çalışmadığından emin olamaz. Daha da vahimi, kullanıcı doğal olarak bankadaki sunucu bilgisayara güvenmek zorunda. Bankaların sunucu bilgisayarları genelde iyi korunduğundan bu güven çok da boşuna değil. Ancak yine de banka sunucuları bir saldırı altında olabilir, çalıştırması gereken programlar değil de belki saldırgan tarafından yereştirilmiş programlar çalışmaktadır. Ya da çalışan programlar, bazı koruma seçenekleri kapatılmış olduğundan yanlış konfigürasyonda çalışıyor olabilir. Benzer şekilde, sunucu bir programın sorunlarından arındırılmış yeni sürümünü değil de eski sürümünü kullanıyor olabilir (insan faktörü güvenlik açıklarının oluşmasında önemli bir rol oynar). Kullanıcının genel güvenlik önlemleri çerçevesinde bu türden bir durumu algılaması ve tespit emesi mümkün değildir.

Başka bir örnek, dağıtık olarak konumlandırılmış gömülü sistem bilgisayar ağlarıdır. Bu türden gömülü sistemler, genelde kontrol ve veri toplama işlerinde kullanılır. Elektrik şebekeleri böyle sistemlere iyi

Anahtar Kavramlar

Güvenilir Hesaplama: Bilgisayarların önceden belirlenmiş spesifikasyonlar çerçevesinde çalışması ve bunun istendiğinde elektronik imza yardımıyla kanıtlanabilmesi
Kriptografi: Güvenli haberleşme ve hesaplama için çeşitli fonksiyon/yapıtaşları/algoritmalar sağlayan şifreleme bilimi
Truva atı: Bir bilgisayar sisteminde kullanıcının isteği ve/veya bilgisi dışında olan/çalışan ve genelde kötü amaçlar için kullanılan bilgisayar programı ya da donanım birimi
Güvenilir Hesaplama Birimi (TPM): Bilgisayar anakartında güvenlik kaynağı olarak kullanılan ve değişik kriptografik fonksiyonları güvenli bir şekilde çalıştıran kriptografik yardımcı işlemci
Elektronik (Sayısal) İmza: Bir dökümanın ya da mesajın belirli bir birey tarafından üretildiği/görüldüğü/onaylandığını ve özgünlüğünü kanıtlayan, söz konusu birey tarafından oluşturulan sayısal mesaj. Mesaj, elektronik imza ve imzalayan kişinin açık anahtarı bilindiğinde imzanın onayı kolayca yapılabilir.
Kriptografik Özüt: Uzun bir elektronik döküman ya da mesajı temsilen özetleyen, sabit uzunluklu ve tersi alınamaz bir fonksiyon tarafından oluşturulan sayısal bir mesaj. Elektronik imza, mesajın ya da dökümanın kendisi yerine özütü kullanılarak oluşturulur.

bir örnektir. Son günlerde ABD'deki elektrik şebekelerine kötü amaçlı yazılımlar (*malware*) yoluyla saldırılar yapıldığına dair söylentiler var. Böyle saldırıların olduğu resmi kaynaklar tarafından doğrulanmadı, ancak birçok uzman söz konusu türden saldırıların mümkün olduğunu ve gerçekleşmesi durumunda ABD'deki yaşamı felç edeceğini belirtiyor. Elektrik şebekelerinin hatasız çalışmasını sağlayan bilgisayarların, doğru programları ve bunların en son sürümlerini çalıştırdığından ve konfigürasyonlarının olması gerektiği gibi olduğundan, yabancı kaynaklı hiçbir yazılımın bu bilgisayarlarda çalışmadığına emin olmak durumundayız. Üstelik bunu çoğu zaman uzaktan yapmak gerekir.

Güvenilir Hesaplama İçin Temel Gereksinimler

- Bilgisayarların herhangi bir anda, olması gereken durumda olup olmadığını anlayabilmeliyiz.
- Bilgisayarlarda çalışan programların özgün ve güvenilir kaynaklardan edinilmiş programlar olması gerekir.
- Bilgisayarlara programların en son sürümlerinin yüklenmiş olduğundan emin olmalıyız.
- Bilgisayarlarda çalışan programların olması gereken konfigürasyonda olduğundan ve gerekli güvenlik mekanizmalarının çalıştığından emin olmalıyız.
- Bilgisayarlarda yabancı kaynaklı hiçbir program çalışmamalı, çalışıyorsa da bunu kolayca algılayabilmeliyiz.

Bütün bu gereksinimleri karşılamak çok da kolay olmayabilir. Örnek olarak, bilgisayarın özgün bir yazılım çalıştırıp çalışmadığının kontrol edilmesi üzerinde yoğunlaşalım. Yazılımın özgün olup olmadığını elektronik imza yardımıyla sınayabiliriz.

Erkay Savaş lisans ve yüksek lisans eğitimini İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Mühendisliği Bölümü'nde sırasıyla 1990 ve 1994 yıllarında tamamladı. 2000 yılında Oregon State Üniversitesi, Elektrik ve Bilgisayar Mühendisliği Bölümü'nden dokotora derecesini aldı. 1993 ve 1997 yılları arasında TÜBİTAK UEKAE'de Araştırıcı ve Uzman Araştırıcı olarak çalıştı, enstitünün kuruluş yıllarında görev aldı. 2000-2002 yılları arasında Almanya'da ve ABD'de çeşitli firmalarda çalıştı. 2002 yılında Sabancı Üniversistesi'nde göreve başladı. Erkay Savaş halen Sabancı Üniversitesi'nde öğretim üyesi olarak görev yapmaktadır.

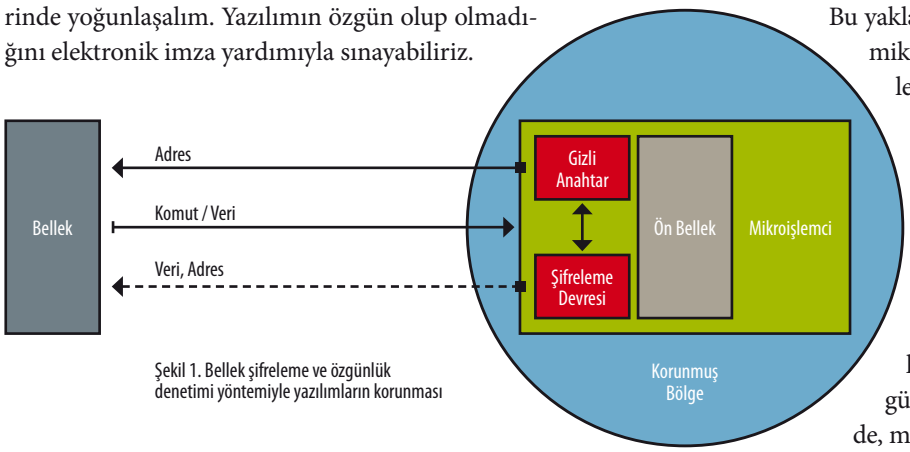
Yazılımı geliştiren taraf, yazılımın çalıştırılabilir kodunun kriptografik özütünü hesaplar ve çıkan sonucu açık anahtarlı bir şifreleme sistemi kullanarak imzalar. Program çalıştırılırken yapılması gereken, programı belleğe yüklemeden önce imzayı yazılımı geliştiren tarafın açık anahtarıyla onaylamaktır. Program özgün ise imza teyit edilir ve yüklenerek çalıştırılır. Çok basit görünüyor. Gerçekten öyle mi?

Akla gelen ilk soru: Programın bir kere yüklendikten sonra değiştirilmeyeceğinden nasıl emin olabiliriz? Daha da ciddi bir soru: Yazılımın özgünlüğünü teyit edecek diğer yazılımın özgünlüğünden nasıl emin olabiliriz? Peki, bu yazılımları belleğe yükleyen ve yöneten işletim sisteminin özgünlüğünden nasıl emin olabiliriz? Çok büyük ve karmaşık yazılımlar olan işletim sistemlerinin birçok hata içerdiği ve bu hataların da saldırılar sırasında kullanıldığı bilinen bir olgu. Peki ya işletim sisteminden önce çalışan BIOS adı verilen, değişik firmalar tarafından geliştirilen yazılımlara güvenecek miyiz?

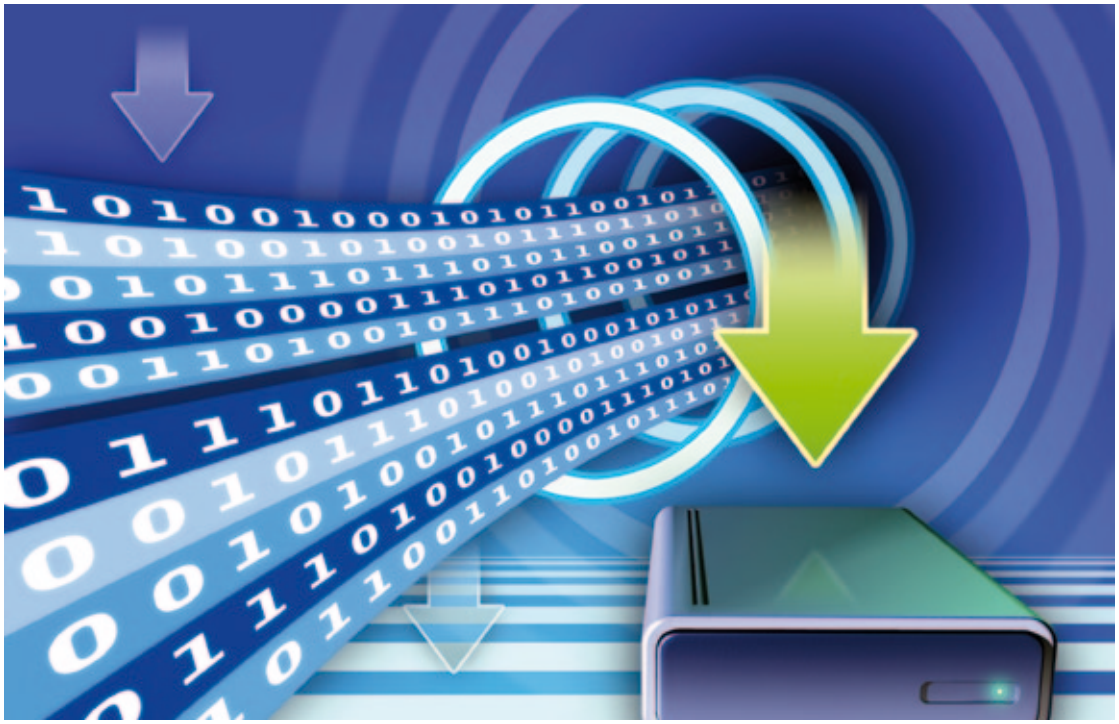
Yukarıda saydığımız yazılımların tümünün hata içerme potansiyeli vardır, tümüne karşı saldırı olduğu da gözlemlenmiştir. Bu durumda çıkarılacak sonuç, ne güvenliğin ne de (yukarıda tanımlandığı anlamda) güvenilirliğin yalnızca yazılım ile sağlanmasının mümkün olduğudur. Bu durumda izlenecek tek yol, donanımı kullanarak bir güven kaynağı yani güven kökü (*root of trust*) oluşturmaktır. Örneğin gizli anahtar donanım önlemleriyle korunarak, donanımda güven kaynağı oluşturulabilir.

Çözüm Donanımda mı?

Bellek şifreleme ve özgünlük denetimi (*memory encryption and authentication*) bu türden yaklaşıma bir örnektir. Amaç, bir mikroişlemci üzerinde çalışan yazılımları ve bunların kullandığı verileri yetkisiz tarafların erişimine ve değiştirmesine karşı korumaktır. Bu yaklaşımdaki varsayım, bir bilgisayar sisteminde mikroişlemci dışındaki birimlerin (özellikle belleğin) güvenilir olmadığı ve güven kaynağının donanımsal tekniklerle korunmuş mikroişlemci yongasında olduğu yönündedir. Şekil 1'de de görüldüğü üzere, şifreleme ve özgünlük denetimi işlemi, donanımsal olarak yine donanımın içerisinde yer alan gizli anahtarla yapılmaktadır. Korunmuş bölge olan mikroişlemciye dışarıdan gelen komut ve veriler, öncelikle şifre çözme ve özgünlük denetiminden geçirilir. Yine aynı şekilde, mikroişlemciden belleğe giden tüm veriler şif-



Şekil 1. Bellek şifreleme ve özgünlük denetimi yöntemiyle yazılımların korunması

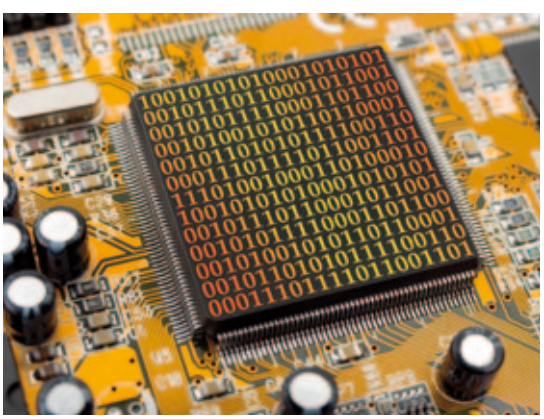


relenir ve kriptografik olarak yetkisiz değişikliklere karşı korunur. Gizli anahtar korunmuş bölgeden çıkmadığından, yapılan işlemlerin güvenli olduğundan emin olabiliriz. Sonuç olarak bu yaklaşımın temel aldığı ilke, mikroişlemcinin güven kaynağı olarak kullanılabileceğidir. Peki bu varsayım ne kadar doğrudur?

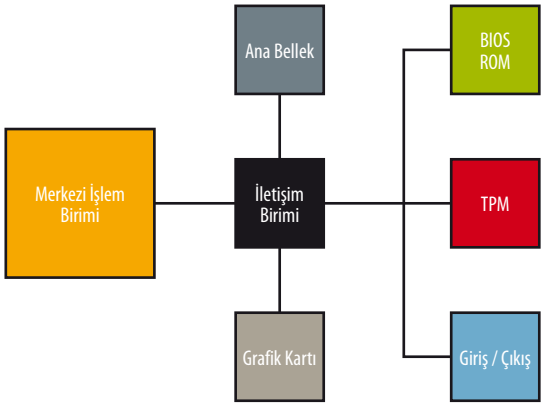
Donanımsal Truva Atları

Donanım tasarlanırken mümkün olan en kuvvetli önlemler alınabilir; böylece güven kaynağı olarak belirlediğimiz donanımı tüm saldırılara karşı dayanıklı hale getirebiliriz. Böylece sorun çözülmüş olur. Ancak daha dikkatli düşünürsek aslında ele almamız gereken başka sorunların olduğu ortaya çıkar. Donanımı kendimiz tasarlayabiliriz, bu bize güven verebilir. Peki donanımı kimin ürettiğini düşündük mü? Donanım üreticisine güvenecek miyiz? Ya da donanımı tasarlarken kullandığımız bilgisayar destekli tasarım (CAD) araçlarına güvenebilir miyiz? Donanım geliştirme araçlarının üçüncü partilerden alınıyor olması, entegre devre üretim tesisleri (FAB) kurmanın milyarlarca dolarlık maliyetlere ulaşması sonucunda üretimin başka ülkelerde gerçekleştiriliyor olması gibi nedenlerle, tasarım ve üretim sürecinde denetimin tam olarak elimizde olmadığını söyleyebiliriz. Donanımın içerisine yerleştirilmiş, fark edilmesi zor, truva atı adını verdiğimiz küçük devreler, gizli ve önemli bilgilerimizi bizden habersiz dışarıya gönderiyor olabilir ya da dışarıdan gelen bir tetikleme mesajı ile etkin hale gelerek sistemin çalışmasını engelleyebilir.

Büyük entegre devre üreticilerinin bu yöndeki yatırımları ve yoğun akademik ilgi, bu senaryoların abartılmış ya da paranoyakça olmadığını kanıtlıyor. Bu konudaki asıl sevindirici gelişme, karşılaştırıcı ve sayıcı gibi küçük ama sözkonusu saldırıların gerçekleştirilmesinde gerekli olan devrelerin bile üretim sonrası testlerle ortaya çıkarılabilir olması. Sayıcı ve karşılaştırıcı truva atı devrelerinin fark edilebiliyor olması bu noktada çok önemli. Saldırının ne zaman gerçekleştirileceğini belirledikleri için bu devrelerin sürekli aktif olması gerekli. Fark edilmelerini mümkün kılan şey de bu. Bu konudaki çalışmaların yeni başladığını ve daha kat edilecek çok yol olduğunu da belirtmek gerek.



Şekil 2. Güvenilir platform biriminin sistem mimarisi içindeki görünüşü

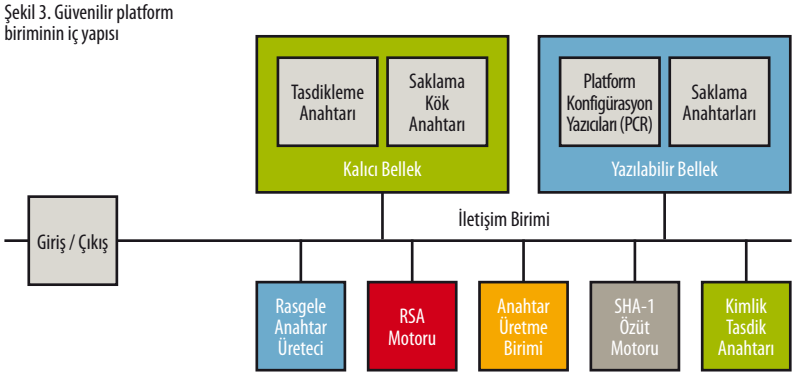


Güvenilir Platform Birimi

Endüstrinin güvenilir hesaplamaya ilişkin yaklaşımını da ele almak gerekir. Aslında güvenilir hesaplama kavramının yaygın bir şekilde gündeme gelmesi ve tartışılıyor olması AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft ve Sun Microsystems gibi firmaların başlattığı TCG (Trusted Computing Group http://www.trustedcomputinggroup.org/) isimli bir endüstri konsorsiyumunun önerdiği ve adını "*trusted computing*" (güvenilir hesaplama) olarak ilan ettiği özel bir teknolojinin gelişmesi sonrasında gerçekleşmiştir. Bu teknoloji, bilgisayar anakartına "güvenilir platform birimi" (Trusted Platform Module - TPM) adı verilen, temel işlevi birtakım kriptografik işlemleri yerine getirmek olan ayrı bir entegre devre konulmasını gerektirir.

Şekil 2'den anlaşıldığı üzere, güvenilir platform birimi (bundan sonra TPM) bir yardımcı işlemci olarak çalışan, temel olarak kriptografik bir işlemcidir. Temel amacı, kriptografik anahtarları korumak ve bazı kriptografik işlemlerin güvenli bir şekilde yapılmasını sağlamaktır. Diğer bir deyişle, TPM devresi yazılımın sağlayamadığı güven kaynağı rolünü oynar. Bu işlev, aşağıda sistemi nasıl koruduğu anlatıldığında daha açık bir şekilde anlaşılacak. Bundan önce TPM'nin iç yapısına kısaca bakmakta yarar var.

Şekil 3. Güvenilir platform biriminin iç yapısı



Şekil 3'te de görüldüğü üzere, TPM'nin temel özelliği gizli anahtarları içerisinde saklaması, RSA ve SHA-1 gibi şifreleme ve özgünlük denetimi işlemlerinde kullanılan standartlaştırılmış kriptografik algoritmaların güvenli bir şekilde çalıştırılmasını sağlamaktır. Kullanıcıya açık, simetrik bir şifreleme algoritması spesifikasyonların zorunlu bir parçası değildir. Bunun nedeni TPM'nin öbek şifreleme işlemlerinde, örneğin dosya şifreleme işlemlerinde kullanılmamasıdır. Bu işlem standart bir simetrik şifreleme algoritmasıyla, yazılım olarak gerçeklenebilir. TPM'nin buradaki katkısı, simetrik şifrelemede kullanılan gizli anahtarı şifrelemek ve ancak sistem güvenilir bir durumdayken, bu anahtarı o anda çalışan yetkilendirilmiş sürecin kullanımına açmaktır.

TPM Güvenilirliği Nasıl Sağlar?

TPM'nin bir çok işlevi var. Yukarıda sözü edilen şifreleme anahtarlarının korunması, elektronik imzalama işlemlerinin yapılması bunlardan bazıları. Ancak şimdi, güvenilir hesaplamayla ilgili olduğundan, yalnızca güvenilir önyükleme (*trusted boot*) işlemini ele alacağız.

Bilgisayarın açma tuşuna bastıktan sonra uzunca bir süre bilgisayarın kullanılabilir hale gelmesini bekleriz. Teknoloji geliştikçe bu sürenin azalacağına artması, bilgisayar teknolojisinde sık rasladığımız bir tuhaflık. Ancak, bilgisayarı ayağa kaldırmak için birbiri ardına çalışan programları düşündüğümüzde bu sürenin uzun olması anlaşılabilir. Özetlemek gerekirse, bilgisayar açıldığında ilk çalışan program (BIOS) ROM adı verilen kalıcı bir bellekten okunur. Bu program, bilgisayarın en basit giriş/çıkış sistemini ayağa kaldırır ve diğer programları çalıştırır: Önyükleme programı, giriş/çıkış cihaz sürücüleri, işletim sistemi çekirdeği, vb. Anlaşılacağı üzere, burada bir zincir yapısı söz konusudur. TPM ile güvenilir hesaplamada, bilgisayarın ayağa kalkması sırasında uygulanan işte bu zincir yapısından yararlanılır.

TPM'li çalışmada, bilgisayar ilk açıldığında BIOS adı verilen programın ancak küçük bir kısmı yüklenir. TPM ve bu kısmi BIOS programı sistemin güven kaynağını oluşturur. Bunlar üreticiler tarafından gerçekleştirildiği için ve yazılım kısmı da yeterince küçük olduğundan saldırılara karşı daha dayanıklıdırlar, hata barındırma olasılıkları daha düşüktür. Kısmi BIOS yüklendikten sonra sıra BIOS programının geri kalan kısmının yüklenmesine gelir. Ancak bu yüklemeden önce kısmi BIOS, yükleyeceği programın 160 bitlik kriptografik özütünü hesaplar ve TPM'nin

içerisindeki platform konfigürasyon yazıcılarından (PCR) birine yazar (bkz. Şekil 3). Çalışmaya başlayan tam BIOS, önyükleme programını yüklemeden önce, yine aynı şekilde bu programın kriptografik özütünü hesaplar ve diğer bir PCR'a bu özütü yazar. Bu işlem kullanıcı programlarının yüklenmesi aşamasına kadar devam ettirilebilir. Dolayısıyla TPM'nin içerisindeki yazıcılarda bilgisayara yüklenmiş programların değiştirilemez özütleri vardır. Bu özütler sorgulanarak, bilgisayarın güvenilir bir yazılım zinciri tarafından açılıp açılmadığı sınanabilir. TPM bir sorgulama ertesinde, PCR içeriklerini gizli anahtarıyla -ki bu anahtar TPM'yi hiçbir zaman terk etmez- imzalar ve sorgulayan tarafa gönderir. Böylece karşı taraf, o bilgisayara güvenip güvenemeyeceğine imza onaylama işleminin sonucuna göre karar verir.

Burada vurgulanması gereken nokta, güvenli hesaplama ile güvenilir hesaplama arasındaki farktır. Güvenli hesaplamada, sistemde daha önceden güvenilirliği tespit edilmiş programlar kullanılmalıdır. Bu kriterlere uymayan programlar çalıştırılmaz, hatta sistem ayağa kaldırılmaz. Güvenilir hesaplamada ise sistemi ayağa kaldırmakta kullanılan programlar isteğe göre değiştirilebilir. Ancak güvenilir hesaplama mekanizması, sistemi ayağa kaldırmak için kullanılan programları elektronik imza gibi kuvvetli bir tasdik yöntemi ile raporlayabilir. Sisteme güvenip güvenmemek kullanıcıya bırakıldığından sistem daha esnektir. Otomobil benzetmesine geri dönersek, zamanında bakıma götürdüğümüzde otomobilin fren sistemi de gözden geçirilir. Otomobili zamanında servise götürüp götürmemek, fren balatalarını değiştirip değiştirmemek, eski ya da kötü parça kullanıp kullanmak tamamen bizim kararımıza bağlıdır. Ama alınacak kararların sonucunda olabileceklerin sorumluluğu da yine bize aittir.

Güvenilir Hesaplama Konusundaki Eleştiriler

Genel olarak bilgisayarlarımızın güvenilir kılınması gerektiği konusunda ortak bir kanı oluşmuştur. Bu amaçla TPM birimleri içeren bilgisayarlar geliştirilmiş ve kullanıma sunulmuştur. Ancak şu anda gerçeklendiği şekliyle, güvenilir hesaplama teknolojisi birçok güvenlik uzmanın eleştirilerine maruz kalıyor. Bu eleştirilerden başlıcası, güvenilirliğin birkaç üretici firmanın tekeline verildiği yönünde. TPM devresinin ve BIOS programının bir kısmının güvenilirliğin kaynağını oluşturduğunu belirtmiştik. Bunları üreten firmalara, çok fazla güvenmek durumunda kalıyor olmamız sakıncalı ve birçok uzmanı da rahatsız ediyor.

Diğer bir eleştiri ise bilgisayar üreticilerinin ve yazılım geliştirme firmalarının, kullanıcının kendi bilgisayarında hangi programları, ne şekilde çalıştıracağı konusunda çok fazla söz sahibi olacak olması. Daha önce belirttiğimiz gibi, bilgisayar çok amaçlı olarak kullanılan bir araç; son yıllardaki teknolojik ve bilimsel gelişmeler de, bilgisayarın farklı alanlarda farklı problemleri çözmek için etkili ve serbest bir şekilde kullanılması sayesinde gerçekleşmiştir. Bilgisayarların bu özelliğini yitirmesine neden olan hiçbir teknolojinin kabul görmesi mümkün görünmüyor. Güvenilir hesaplama konusu, bilimsel/teknolojik bir araştırma alanı olarak henüz emekleme aşamasında. Genel kabul görecek teknolojilerin geliştirilmesi ya da varolanların bu yönde evrilmesi bu araştırmaların kaçınılmaz bir sonucu olacak.

Kaynaklar

Agrawal, D., Baktır, S., Karakoyunlu, D., Rohatgi, P. ve Sunar, B., "Trojan Detection Using IC Fingerprinting", IEEE Symposium on Security and Privacy (SP), s. 296-310, Mayıs 2007.

Durahim, O. A., Savaş, E., Sunar, B., Pedersen, T. B. ve Kocabaş, O., "Transparent Code Authentication at the Processor Level", *IET Computers & Digital Techniques* (yayımlanacak).

Gassend, B., Suh, E. G., Clarke, D. E., Dijk, M. van ve Devadas, S., "Caches and Hash Trees for Efficient Memory Integrity", Ninth International Symposium of High Performance Computer Architecture (HPCA 2003) Kitapçığı, s. 295–306, Şubat 2003.

"Intel New Release", http://www.intel.com/pressroom/archive/releases/20071025corp.htm linkinden erişilebilir.

Lee, R. B., Kwan, P. C. S., McGregor, J. P., Dwoskin, J. S. ve Wang, Z., "Architecture for Protecting Critical Secrets in Microprocessors", The International Society for Computers and Their Applications, s. 2–13. IEEE Computer Society, 2005.

Mitchell, C., *Trusted Computing*, Institution of Electrical Engineers, 2005.