Bilişim Güvenliği: Güvenli Hesaplama

İlhan Kaya[1], Şerif Bahtiyar[2]

[1] İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, İstanbul

[2] Progress Ar-Ge Merkezi, Provus Bilişim Hizmetleri A.Ş., Şişli, İstanbul

kayailh@itu.edu.tr, serif.bahtiyar@provus.com.tr

Özet: Geleneksel bilgi teknolojilerinin açıklarını kullanan düşmanlar, bu sistemlere saldırıda bulunmaktadırlar. Bu saldırıları engellemek ve güvenliği arttırmak için kullanılan bir yöntem de güvenli hesaplama teknolojisidir. Bu teknolojiyi kullanan bilgi sistemleri, birçok zararlı yazılımın ve düşmanın saldırılarına karşı daha korunaklıdır. Bu çalışmamızda, güvenli hesaplamayı araştırarak, bu konu ile ilgili potansiyel araştırma konularını işaret etmeyi amaçladık.

Anahtar Sözcükler: Güvenli Hesaplama, Güvenlik, Bilgi Teknolojisi

IT Security: Trusted Computing

Abstract: Traditional information system technologies contain many security vulnerabilities that ensure an adversary to attack such systems. Trusted computing technology is used to enhance security of information systems and prevent many attack vectors. Information systems that employ trusted computing systems are less prone to attacks of malicious software and adversaries. In this paper, we have investigated trusted computing to point out potential research challenges regarding information security.

Keywords: Trusted Computing, Security, Information Technology.

1. Giriş

Güven kavramını basitçe ele alırsak, birisinin davranışlarının beklentilerimize göre şekilleneceğinden emin olmamız durumunda o kişiye güveniriz. Karşılıklı güvenin sağlanması için önceki deneyimlere dayanan ilişki veya zaten güvenilen üçüncü bir kişinin garantisi gerekmektedir. Güven ilişkisini, maddi veya manevi bilgi akışının güven duygusu içerisinde sağlanmasına dayandırmamız gerekir. Temel olarak güven ilişkisini şunlarla bağdaştırabiliriz:

- Gizliliğin sağlanması (confidentiality)
- Bütünlüğün sağlanması (integrity)
- Erişimin sağlanması (availability)
- Kurtarmanın sağlanması (recoverability)

Günümüzde bilgisayarları kullanarak gerçekleştirdiğimiz işlemlerin hem sayısı ve çeşidi hem de bu işlemlerin ciddiyeti artıyor.

Bu çalışmamızda, güvenli hesaplamayı araştırarak, bu konu ile ilgili potansiyel araştırma konularını işaret etmeyi amaçladık. Çalışmamızın ikinci bölümünde güvenli hesaplamayı anlattık. Üçüncü bölümü güvenli hesaplama grubu için ayırdık. Sonraki bölümde güvenilir hesaplama birimini açıkladık. Son bölümde, bildirimizi tamamladık.

2. Güvenli Hesaplama

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?

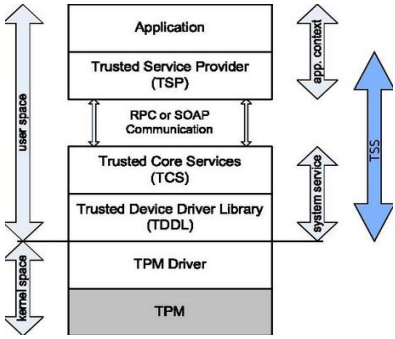
Teknoloji dünyasında her geçen gün giderek artan bir şekilde bilgisayarlar (Desktop, PC, Mobile Cihazlar ve diğer işletim sistemi olan makineler) arasında veri paylaşımı gerçekleşmektedir. Bu paylaşım ve iletişim gerçekleşirken verinin doğru ve güvenli kaynaktan geldiğine veya doğru kaynağa doğru şekilde güven içinde iletildiğine karar vermek için Güvenli Hesaplama kullanılır. Bütün bu işlemlerin oldukça hızlı bir şekilde güvenlik protokollerine uyularak gerçekleştirilmesi gerekmektedir. Güvenli Hesaplama ile işletim sistemleri daha güvenli bir hal alırlar ve dışarıdan gelebilecek zararlı yazılımları daha iyi bir şekilde denetleyebilirler. Bilgisayara gerekli donanımın eklenmesi ve bu donanımın güvenli ve doğru şekilde çalışmasını sağlayacak yazılım ile işletim sistemlerinde Güvenli Hesaplama gerçekleştirilir [5]. Güvenli Hesaplamaya sahip bir işletim sistemi ile uzaktaki bir bilgisayara bağlanıp güvenli bir şekilde, güven içinde, iletişim kurabilirsiniz.

Güvenli Hesaplama 1990'ların sonundan günümüze kadar, özellikle son 4-5 yıl içinde çıkan çok sayıda güvenlik odaklı problemin (Virüs ve solucanlar, istenmeyen eposta (spam), uygulamaların kırılması) çözümünde kullanılmaktadır. Güvenli Hesaplama, kötü amaçlı yazılımlara karşı işletim sistemimizin daha güvenli olmasını sağlarken, işletim sistemini aynı hassasiyet içinde korur [3]. Günümüzde, bilgi teknolojilerinin açıkları Güvenli Hesaplama kullanılarak giderilmeye çalışılmaktadır.

Güvenli Hesaplama aynı zamanda yüksek güvenlik gerektiren özel veya kurumsal firmalarda kurumsal verileri, platformların ve ağların korunması için siber savunma sistemleri ile birlikte kullanılır.

Bütün bu işlemleri gerçekleştiren Güvenli Hesaplama bilişim dünyasının önde gelen donanım ve yazılım üreticileri tarafından oluşturulmuş Trusted Computing Group

tarafından belirlenen politikalar ve modüller ile gerçeklemeye çalışılmaktadır. Şekil 1' de görüldüğü gibi Güvenli Hesaplama donanımsal ve yazılımsal olarak çeşitli aşamalardan oluşmaktadır.



Şekil 1. Güvenli Hesaplama yapısı [5].

2.1 Güvenilir Bilgisayar

Kullandığımız diğer tüm cihazlarda olduğu gibi, bilgisayarın da komutlarımıza uymasını ve bunu bize söylenen şartnamelere uygun bir şekilde gerçekleştirmesini bekleriz [1]. 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.

2.2 Güvenli Hesaplama Gereksinimleri

Gereksinimler aşağıda listelenmiştir:

- Bilgisayarın olması gereken durumda olduğunu anlamak
- Bilgisayardaki yazılımların güvenilir kaynaklardan edinilmiş olması
- Yazılımların son sürümlerine güncellenmiş olması
- Bilgisayardaki güvenlik mekanizmalarının çalışır durumda olması
- Bilgisayarda yabancı kaynaklı yazılım çalışmaması

2.3. Güvenli Hesaplama Faydaları

- Çeşitli saldırılara karşı kritik verilerinizi ve sisteminizi korur.
- Güvenli kimlik doğrulama ve güçlü şifre anahtarlamaları yapmak için gerekli sertifikaları barındırır.
- Makinenizin kimliğini ve bütünlüğünü korur.
- Yasal uyumluluğu sağlamak için tabanı güvenli donanım oluşturulmasına yardım eder.

3. Güvenli Hesaplama Grubu

Çoğu, alanının en büyükleri arasında gösterilen (HP, IBM, Intel, Microsoft, Sony ve Sun Microsystems gibi) 160'tan fazla donanım ve yazılım firmasının bir araya gelerek oluşturduğu Güvenli Hesaplama Grubu (Trusted Computing Group - TCG), Güvenli Hesaplama ile ilgili teknolojiler geliştirilirken hangi standartların ve mimarinin uygulanacağına karar verir. TCG çoklu platformlar, çevresel ve diğer aygıtlar arası donanım blokları ve yazılım arabirimleri oluşturmayı içeren donanım-etkin güvenilir hesaplama ve güvenlik teknolojileri gibi açık standartlar geliştirmeyi ve tanımlamayı amaçlayan kar amacı gütmeyen bir yapılanmadır. Bu grup, tasarım, uygulama ve kullanım için güvenliği ve gizliliği koruyacak taahhütler (Best Practices and Principles) yayınlamaktadır. Bunu birden fazla platformda tanımlanan ve geliştirilen aygıtlar arasında güvenlik teknolojilerini ve açık standartların belirlenmesi için kullanır.

TCG özellikle gelecekte üretilecek cihazların standartlarına odaklanmaktadır. Çünkü yeni cihazlarda güvenlik açığı daha fazla olabilmektedir [2]. Bu grubun çalışmalarından biri ve en önemlisi, Güvenilir

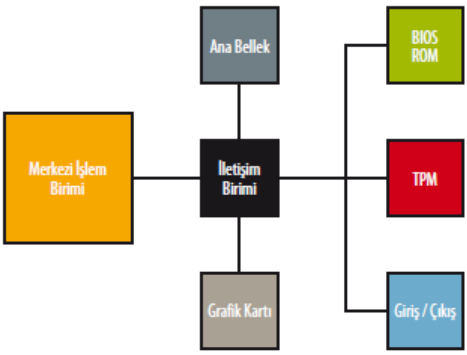
Platform Birimi (Trusted Platform Module - TPM)' dir [3].

4. Güvenilir Platform Birimi

TCG tarafından ortaya konan bir çalışma olan Güvenilir Platform Birimi (TPM) günümüzde birçok bilgisayar üzerinde hazır gelen donanım tabanlı bir çeşit güvenlik ve kriptografi yongasıdır. Bu yonga içerisinde dijital sertifika, kriptografik anahtarlar, parolalar ve benzeri birçok gizli bilgi barındırılır.

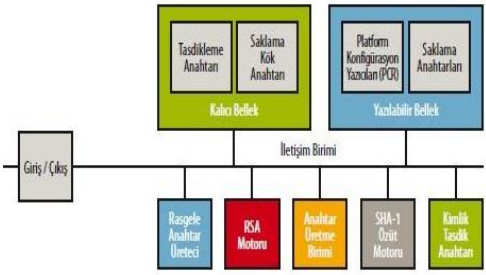
4.1 Güvenilir Platform Biriminin İşlevi

TPM'in birçok işlevi vardır. Bu işlevlerden bazıları anahtar yönetimi, üzerinde çalıştığı PC'nin kimliğini doğrulama, elektronik belgeler ve e-postalar üzerinde güvenli elektronik imzalama, şifreleme, şifre çözme işlemlerini gerçekleştirmedir. Tam-sürücü şifrelemeyi yönetme, çok yönlü doğrulamada, ikinci faktör olarak görev yapma ve üzerinde bulunduğu bilgisayarın güvenliğini ve bütünlüğünü değerlendirmeye yardımcı olma diğer bazı işlevlerdendir. TPM, bilgisayarın ana kartına temel işlevi birtakım kriptografik işlemleri yerine getirmek olan ayrı bir bütünleşmiş devre konulmasını gerektirir.



Şekil 2. TPM'nin işletim sistemi mimarisindeki yeri [3].

TPM, bir yardımcı işlemci olarak çalışan temel olarak kriptografik bir işlemcidir. Ana işlevi, kriptografik anahtarları korumak ve bazı kriptografik işlemlerin güvenli bir şekilde yapılmasını sağlamaktır. Bir diğer bakış açısı ile TPM, devresi yazılımın bir türlü sağlayamadığı güven kaynağı rolünü oynar.



Şekil 3. TPM iç yapısı [3].

Şekil 3'te de görüldüğü üzere, TPM'nin temel özelliği gizli anahtarları içerisinde saklaması. Diğer bir değişle, 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 şartnamelerin 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.

4.2 Güvenliğin Sağlanması

Şifreleme anahtarlarının korunması, elektronik imzalama işlemlerinin yapılması gibi TPM'nin birçok işlevi vardır. Bu

işlevlerin en önemlilerinden biride güvenilir önyüklemedir. Gün geçtikçe yeni çıkan teknolojilerde bilgisayarların açılma süresinin kısalması gerekirken uzadığı fark edilmiştir. Bunu sebebi, arka planda çalışmaya başlayan onlarca programdır. Normal olarak bilgisayarı ilk çalıştırdığımızda, ROM içinde bulunan BIOS bilgisayarın giriş-çıkış işlemlerini yürütmeye başlar ve diğer programları çalıştırır.

TPM'li bir bilgisayar açılışında ise ilk olarak BIOS'un küçük bir kısmı yürütülür. BIOS'un bu kısmı ve TPM bilgisayarın güven kaynağını oluştururlar. 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. TPM bir sorgulama ertesinde, gerekli kısmı imzalar ve sorgulayan tarafa gönderir. Böylece karşı taraf, o bilgisayara güvenip güvenemeyeceğine imza onaylama işleminin sonucuna göre karar verir.

5. Sonuç

Genel olarak bilgisayarlarımızın güvenilir kılınması gerektiği konusunda ortak bir kanı oluşmuştur. Bunu temel sebebi, bilgisayarların bize ait bilgileri içeriyor olmasıdır. Güvenli Hesaplama ile kendimizi ve bilgisayarımızı göreceli olarak güven içinde hissedebiliriz. Güven, TCG tarafından çıkarılmış ve çıkacak olacak standartlar doğrultusunda TPM ile gerçekleştirilmektedir. Bu standartlar ile bilgisayar üreticilerinin ve yazılım geliştirme firmalarının, kullanıcının kendi bilgisayarında hangi yazılımları, ne şekilde çalıştıracağı konusunda çok fazla söz sahibi olacağı aşikârdır. Bu durum mevcut TCG tabanı güven sistemleri ile ilgili ayrı bir düşündürücü konudur.

Teşekkür

Bu çalışma EUREKA ITEA2 projesi ADAX (proje no. 10030) ve TEYDEB projesi AKFİS (proje no. 1130018) tarafından desteklenmiştir.

6. Kaynaklar

[1] Fournaris, A. P., "Toward Flexible Security and Trust Hardware Structures for Mobile-Portable Systems", **IEEE Latin America Transactions**, 1719-1722, (2012).

[2] Metke, A. R., Ekl, R. L., "Security Technology for Smart Grid Networks", **IEEE Transactions on Smart Grid**, 99-107, (2010).

[3] Cabiddu, G., Cesena, E., Sassu, R., Vernizzi, D., Ramunno, G., Lioy, A., "The Trusted Platform Agent", **IEEE Software**, XXVIII: 35-41, (2011).

[4] Mooseop, K., Hongil, J., Youngsae, K., Jiman, P., Youngsoo, P., "Design and implementation of mobile trusted module for trusted mobile computing", **IEEE Transactions on Consumer Electronics**, 134-140, (2010).

[5] Huanguo, Z., Yi, M., "Trusted computing and information security", **Communications**, 9-10, (2013) **.**