Güvenli Önyükleyici ile Güvenlik Seviyenizi Artırın

Bahadır Demircioğlu

Ocak, 2013

Ben Secure Boot Bootloader'ı "Güvenli Önyükleyici" olarak adlandıracağım yazımda. MacOS'nin yıllardır benzerini kullandığı güvenlik optimizasyonu artık bütün Linux dağıtımlarında olacak. Güvenli Önyükleyici yazılımsal bir yön olmasına rağmen bazı donanımsal özellikler de istemektedir. Tabii iş bu kadarla da bitmiyor; donanımsal isteklerin yanında BIOS üzerinde de çeşitli istekleri var Güvenli Önyükleyicinin. Bildiğimiz eski klasik BIOS ile Güvenli Önyükleyici seçeneğini kullanamıyoruz. Kullanabilmemiz için anakartımızın UEFI BIOS 2.3.1 ve üstü olması gerekmektedir. Buradan kısaca şunu çıkarabiliriz: Güvenli Önyükleyici yazılımsal bir özellikten ziyade UEFI, yani donanımsal bir özelliktir.

Artık konuya giriş yaptığımıza göre Güvenli Önyükleyicinin ne işe yaradığından bahsedelim. Kısaca tek cümleyle söylemek gerekirse Güvenli Önyükleyici bilgisayarımızda sadece yetkilendirilmiş işletim sisteminin başlatılmasını sağlamaktadır.

Bu noktada sanırım biraz da klasik olarak bilgisayarın ilk açılış prosedürlerinden bahsetmem gerekecek. Bilgisayarın ilk açılışında BIOS devreye girer. İşletim sistemine görevi devredene kadar yapılması gereken işleri BIOS yapacaktır. Bu esnada donanımların sağlamlığını test eder. Her şey olağan ise görevini işletim sisteminin önyükleyicisine bırakır. Görevi devralan işletim sistemi de kendi prosedürlerini uygulayarak açılır. Her işletim sisteminin kendine özgü bir önyükleyicisi bulunmaktadır.

BIOS işi devredene kadar işlemlerin hiçbir kontrolden geçmediğini gördük. İşte Güvenli Önyükleyici burada işe biraz daha güvenlik katıyor. Güvenli Önyükleyicide bu güvenlik şu şekilde sağlanıyor: BIOS görevini işletim sistemine devretmeden önce önyükleyiciye gömülmüş olan dijital bir imzayı kendi içerisinde bulunan veri tabanındaki imzalar ile karşılaştırıyor. İşletim sisteminin önyükleyicisindeki imza ile uyuşma sağlanırsa işletim sistemi devreye giriyor. Eğer imza uyuşma sağlanmazsa yüklemenin önüne geçilmiş oluyor. Burada şu akıllara gelebilir: Güvenli Önyükleyici sayesinde bazı işletim sistemlerinin bilgisayarlara yüklenmesinin önüne geçilebilir. Yıllardır Mac bilgisayarlara Machintosh'dan başka işletim sisteminin yüklenememesi gibi. Burada asıl amaç bu değil. Buradaki amaç Rootkit'lerden savunmayı sağlama ve yetkisiz işletim sistemlerinin yüklenmesinin önüne geçmek.

Şöyle bir örnek verelim: Bilgisayarınızı kapatıp gittiniz ve içinde öenmli verileriniz var. Bir kişi sahip olduğu canlı işletim sistemi yüklü usb ile sisteminiz korumalı dahi olsa açıp içinden verileri kopyalayabilir. Bunun önüne geçmemizin yolu anlattığım gibi Güvenli Önyükleyici kullanmaktır. Güvenli Önyükleyici tamamen kişinin inisiyatifine bağlıdır. İstediğiniz taktirde bu özelliği kullanmama gibi bir hakkınız da bulunmaktadır.