Kobil mIDentity…

written by Mert SARICA | 27 January 2010

Geçtiğimiz günlerde Kobil mIDentity USB aygıtını inceleme fırsatını yakaladım. Nedir bu midentity diyecek olursanız kabaca birden fazla işlemi güvenli bir şekilde gerçekleştirebilen bir aygıt olarak piyasaya sürülmüş, şifrenizi, sertifikanızı, OTP'nizi, doman şifrenizi vb.lerini sadece pin girerek sistemlere kendinizi doğrulatmanızı sağlayan akıllı bir aygıt olarak düşünebilirsiniz. Kullanım alanlarına bakacak olursak, internet bankacılığına girişten, iş e-postalarınızı ve dosyalarınızı şifrelemeye ve imzalamaya kadar bir çok alanda kullanabiliyorsunuz. Ürün hakkında daha detaylı bilgi almak için buraya tıklayabilirsiniz.

Gelelim bizi asıl ilgilendiren kısma, bu kadar marifetli bir aygıt olmasına rağmen her işlemi aynı ölçüde güvenli olarak yerine getirebiliyor mu ?

İncelediğim aygıt demo aygıtı olduğu için PIN'i önceden belirlenmiş, sertifikaları yüklenmiş ve autorun ile çalıştırıldığında Kobil tarafından hazırlanmış bir demo sayfasına yönleniyor ve bu sayfada aygıtı test etmeye imkan tanıyordu.

Demo sayfasına girdikten sonra Kobil'in reklam sayfası ile karşılaşıyorsunuz ve bu sayfayı geçtikten sonra hemen karşınıza aygıtı denemek için türlü sayfalar sizi karşılıyor, güvenli giriş, dosya şifreleme, pin değiştirme ve puk değiştirme.

Güvenli giriş, internet bankacılığında kullanılan mobil imza ile aynı olduğu için ve size sunucu tarafından verilen bir metni aygıt ile imzalayarak karşı tarafa göndermeniz istendiği için sunucu ile aygıt arasına girmeniz ve imzalanan metni değiştirmeniz ve sunucuya göndermeniz durumunda haliylen hatalı imza uyarısı ile karşılaşıyorsunuz, bu kısımda herhangi bir sorun ile karşılaşmadım.

Dosya imzalama ise uygulama üzerindeki göz at butonuna basarak diskiniz üzerinde yer alan herhangi bir dosyayı seçiyorsunuz, pin girerek aygıta imzalatıyorsunuz ve daha sonrasında sunucuya gönderdiğinizde sunucu dosya ile imzayı karşılaştırarak sizin bu dosyayı imzaladığınızı teyit etmiş oluyor. Güvenli girişte olduğu gibi işlem sunucu tarafından başlatılmıyor aksine bu defa istemci imzalama işlemini başlatıyor ve aygıt ile imzalayıp gönderiyor. Aynen bende şuan sizin aklınızdan geçirdiğiniz gibi "istemci tarafından

başlatılan bir işlem bir şekilde bypass edilir mi?” düşüncesi ile işe koyuldum ve bir trojan hayal ettim.

Trojanımız biz X dosyasını seçsekte o gidip memoryden gidip Y dosyası ile değiştirse, ön yüzde X dosyası gözükmesine rağmen arka tarafta Y dosyası imzalansa ve sunucuya gönderilse bizim haberimiz olur mu ? Sunucu size sen bu dosyayı imzaladın diye transfer işlemi tamamlandıktan sonra gösterse dahi trojan Man-in-the-Browseryeteneğine sahipse sunucu tarafından gelen yanıtıda değişterecek ve haberimiz olmayacaktır.

İstemci tarafında başlatılan ve gerçekleştirilen dosya imzalama işleminde bu sorun var ise peki ya istemci tarafında başlatılan diğer bir işlem olan internet bankacılığı işlem imzalamada da aynı sorun yaşanır mı yaşanmaz mı sorusunun yanıtını size bırakıyor, Kobil’in kısa zaman içerisinde bu tür basit müdahaleleri engellemek için ek kontroller uygulamasını ümit ediyorum. (Not: Kullandığım aygıtta yer alan uygulamalar 2008 yılındaki sürüme ait, belki bu geçen zaman zarfında bu sorunlar ortadan kalkmış olabilir, bu nedenle son sürüme güncellemenizi her durumda öneriyorum.)

Sonuç olarak dosya imzalamayı gerçekleştiren bir trojan tabiiki yazmadım ancak pratikte nasıl gerçekleştirilebileceğine dair ufak bir video hazırladım, iyi seyirler…

[2010-01-28 19:03:46] Güncelleme: mIDentity’nin yeni sürümünde memory’e müdahale edilmesi engellenmiş, kontrol ettim ancak aşmak için uğraşmadım. İmzalama işlemi işletim sistemi üzerinden başlatıldığı sürece her zaman aşılma riski olacaktır.