RFID klonlarının yarattığı güvenlik sorunları (2)

ÇETİN KAYA
KOÇ

RFID etiketine açık anahtarlı yeniden şifreleme görevi yüklemek ne kadar gerçekçi? Peki bu protokol gerçekten olabilecek en iyi çözüm mü?

RFID etiketlerinin güvenlik sorunlarından bir tanesi de klonlama. Klonlamayı zorlaştıracak metodlar, ne yazık ki "astarı yüzünden daha pahalı" çözümler kategorisinden. Bu yüzden şimdi genel eğilim klonlamaya izin vermek. RFID etiketi kimlik belirleyici sayıyı (identifier) tutuyor ve arzu eden herkes bu etiketin klonunu elde edebilir. Ancak elde ettiğiniz şey RFID etiketinin o andaki hali; yani her durumda geçerli olan evrensel bir klon elde etmiyorsunuz.

Arka plandaki protokol, iki adımlı özel bir kimlik doğrulama metodu yardımıyla sizin kedinizin kapıdan girmek istediğini anlıyor. Bu protokolun detaylarını bu yazımızda açıklayacaktık: Protokol "yeniden şifreleme" metoduna dayanıyor. Bir sistem açık anahtarlı şifreleme algoritması ile etiketin kimliğini şifreliyor. RFID etiketi bu şifreyi hafızasında tutuyor ve onu yayıyor. Böylece etiketin kimliğinden emin olmak isteyen biri, bu şifre değerini sisteme sunup, sistem gizli anahtarı vasıtası ile kimlik doğrulamasını sağlayabilir. Ancak RFID etiketi belli aralıklarla (mesela birkaç günde bir) rastgele bir sayı kullanarak ve sistemin açık anahtarı ile kimliğini yeniden şifreleyip bu sayıyı hafızasına koyuyor, böylece kimliği aynı kaldığı halde kimlik sayısı yenilenmiş oluyor. Kimlik doğrulayıcı aynı adımları kullanarak ve yine sistemin açık anahtarlı algoritması ile gerçek RFID etiketinin kimliğini tekrar doğrulayabilir. Ancak klonlanmış RFID etiketini elde eden kişi eskimiş şifreli kimlik değeri kullanacağı için başarılı olamaz; yeni bir klon üretmesi gerekir.

Böylece klonlayan saldırganın her zaman birkaç adım önünden giderek "sahte kimlikli kedinin" kapıdan girmesini engellemiş oluyoruz. Peki bu protokol gerçekten olabilecek en iyi çözüm mü? RFID etiketine açık anahtarlı yeniden şifreleme görevi yüklemek ne kadar gerçekçi? Ben bu konuya bir süre ara verip, önümüzdeki haftalardaki yazılarımda size RFID etiketlerinin mahremiyet sorunlarından bahsedeceğim.

koc@cryptocode.net