RFID klonlarının yarattığı güvenlik sorunları (1)

ÇETİN KAYA KOÇ

RFID etiketlerinin güvenlik sorunlarından bir tanesi de klonlama.

Basit bir RFID etiketi, prensip olarak hafızasında tuttuğu kimlik belirleyici sayıyı (identifier) yaymaktan başka bir iş yapmadığı için, onun bir kopyasını yapmak çok kolay. Başka bir RFID etiketine bu sayıyı yazmamız yeterli. RFID etiketlerinin erişim kontrolu uygulamalarında, özellikle tek adım kimlik doğrulama (one-factor authentication) metodu kullanılıyorsa, klonlama olasılığı bir güvenlik tehlikesi arzediyor. Klon etiket aslı sanılacağı için, kapıdan içeri girecektir. Evcil hayvanları ve hatta insanları etiketlemek için RFID kullanılacağı için, otomatik kontrollu kapıdan sizin kedinizin yerine bir hırsız bir kedinin girmesi söz konusu!

Peki bunu nasıl önleyeceğiz. Bir fikir klonlamayı zorlaştırmak. Örneğin, bir challenge-response veya zero-knowledge protokolü ile RFID cihazı, içindeki gizli bilgiyi vermeden o bilgiye sahip olduğunu ispat edebilir. İlerdeki yazılarımda böyle protokolleri anlatmayı planlıyorum, ancak şimdilik özet olarak şunu söyleyeyim: bu tip protokoller açık-anahtarlı şifreleme sistemlerine, sayılar ve karmaşıklık teorilerine dayanıyor. Bunları RFID yongalarına sığdırmak, RFID etiket teknolojisinin prensiplerine, yani ucuz ve küçük olma ve az enerji kullanma özelliklerine aykırı.

Üstelik klonlamanın zorlaştırılması saldırganın fiziksel olarak RFID etiketini ele geçirmesine engel değil. Yani kedinizi ele geçirip, boynundan RFID etiketini alabilirler. RFID etiketinin deri altına implantasyonu durumunda ise daha vahim sonuçlar çıkabilir. Biyometrik sistemlere yapılan fiziksel saldırılar gibi (örneğin, saldırganın kullanıcının parmağını kesip kullanması gibi), implantasyon halindeki RFID etiketini almak için kedinizi yaralamaları ve hatta öldürmeleri söz konusu. (Bu yazının tonu için kediseverlerden özür dilerim, ancak saldırıları anlatmak için örnek vermek zorundayım.)

Başka bir çözüm var mı, diye soracaksınız. Öyle gözüküyor ki en iyi çözüm klonlamaya izin vermek. Yani klonlamayı zorlaştırmayacaksınız. RFID etiketi kimlik belirleyici sayıyı tutacak ve arzu eden herkes bu etiketin klonunu kolaylıkla elde edebilecek. Ancak arkaplandaki protokol, iki adımlı bir kimlik doğrulama (two-factor authentication) metodu yardımıyla sizin kedinizin kapıdan girmek istediğini anlayacak. Bu protolun detayları bir sonraki yazımızda.

koc@cryptocode.net