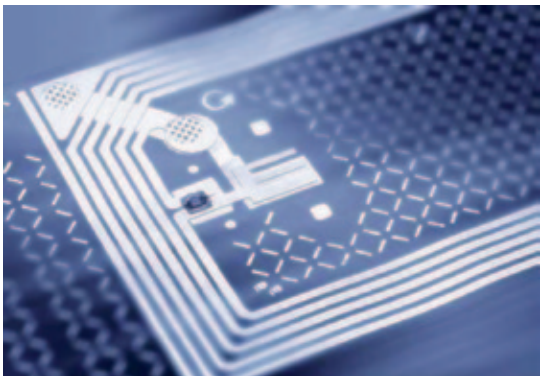
Oğuzhan Vıcıl

Dr., Bilimsel Programlar Uzmanı,
TÜBİTAK Bilim ve Toplum
Daire Başkanlığı

Temassız Kredi Kartları Güvenli mi?

Birkaç sene önce gelişmiş ülkelerde başlayan temassız akıllı kredi kartları kullanımı, ülkemizde de kullanım hızı ve kolaylığı ile birlikte hayli yaygınlaştı. Köprü ve otobüs gişelerinde, deniz otobüslerinde ve ayaküstü restoranlarda artık bozuk para ve bilet yerine bu kartları gösterip geçmek mümkün. Ama her yeni teknoloji gibi bu teknoloji de kullanım kolaylıklarının yanı sıra bir takım güvenlik endişelerini de beraberinde getiriyor.

Peki, pek çoğumuzun yeni yeni tanımaya başladığı bu teknoloji ne kadar güvenli?



Kredi kartı pazarı tüm dünyada giderek büyüyor ve Türkiye bu pazarda son yılların en fazla büyüme gösteren ülkelerinden biri. Bu özelliği Visa ve MasterCard gibi dünya devlerinin de dikkatini çekmiş olacak ki artık Türkiye önemli stratejik ülkeler arasında yer alıyor. Birçok teknolojik yeniliğin ilk uygulama alanlarından biri ülkemiz oluyor. Bu yeniliklerden biri olan temassız kredi kartı teknolojileri, MasterCard-PayPass ve Visa-PayWave ile ülkemizde de kısa bir süre içinde birçok banka tarafından kullanıcıların hizmetine sunuldu. Bu teknoloji, PayPass veya PayWave özellikli kredi kartlarının, belirli bir tutarın altındaki (şu an için 35 TL) alışverişlerde özel olarak tasarlanmış POS cihazı okuyucularına yaklaştırılarak şifre girilmeden ödeme yapılması prensibine dayanıyor. Kullanım kolaylığı ve zaman kaybını önlemesinin yanı sıra agresif reklam kampanyalarının da etkisiyle olacak, bugün ülkemizde iki milyona yakın temassız kredi kartı dolaşımda.

Kart sahipleri açısından nakit ve bozuk para derdinden kurtulma anlamına gelen bu teknoloji, aynı zamanda işlem süresini kısalttığı için ödeme kuyruğunda bekleme çilesine de bir çözüm getiriyor. Ülkemizde temassız kredi kartları ayaküstü restoranlar, kafeler, sinemalar, gazete bayileri gibi küçük tutarlı alışveriş yapılan, temassız okuyucuya sahip üye işyerlerinde, anlaşmalı illerdeki belediye otobüslerinde ve taksilerde, bütün otoyol ve köprülerdeki KGS gişelerinde ve İDO turnikelerinde kullanılıyor.

Yeni yeni tanımaya başladığımız, kullanım alanı sürekli genişleyen ve kullanıcılar açısından büyük kolaylık sağlayan bu teknoloji ister istemez bir takım endişeleri de beraberinde getiriyor. Güvenlikle ilgili potansiyel açıkları daha iyi anlayabilmek ve yorum yapabilmek için öncelikle bu teknolojiyi kısaca tanıyalım.

Akıllı Kredi Kartları

Kredi kartlarını imzalı kullandığımız dönemlerde kişisel bilgiler manyetik şeritler üzerinde depolanıyordu. Dünyada ve ülkemizde birkaç sene önce uygulamaya geçen Çip ve Şifre (Chip & PIN) ve Temassız (Contactless) kredi kartlarında ise kişisel bilgiler daha güvenli korunma sağlayan çipler üzerinde depolanıyor. Karta gömülü çipler ve üzerlerindeki özel yazılımlar sayesinde, bu kartlar gerçekleştirmeleri istenen fonksiyonları (büyük miktarda veri depolama, şifreleme, karşılıklı kimlik doğrulama, vs.) akıllı bir şekilde yerine getirme kabiliyetine sahip. Bu teknolojiye Akıllı Kart (Smart Card) teknolojisi deniyor. Temassız kredi kartlarını standart kredi kartlarından ayıran en temel fark, temassız kartların çip üzerindeki kişisel bilgileri okuyucuya RFID teknolojisindekine benzer şekilde radyo yayını ile iletmesi. Çip ve Şifre'li kartlarda ise çip üzerindeki bilgiler karta uyumlu okuyucuya takılarak doğrudan temas ile okunuyor.

Temaslı akıllı kart teknolojileri uluslararası ISO/IEC 7816 standardına uyumlu iken, temassız akıllı kredi kartları için bu teknolojinin uyumlu olması gereken standart ISO/IEC 14443'tür. Bu standart 10 cm'den daha kısa mesafede çalışan temassız akıllı kartlar için geçerli olan uluslararası standarttır ve şunları içerir: Radyo yayın frekansı 13,56 MHz, fiziksel teknik özellikler, radyo frekans gücü ve sinyal arayüzü, radyo dalgalarının iletimi ve çakışma önleyici protokoller. Burada ufak bir hatırlatma yapalım: Ülkemizde dolaşımda olan temassız kredi kartları, aynı zamanda temaslı akıllı kart özelliğine de sahip olduğu için her iki standarda da uyumlu olması gerekiyor.

Ülkemizde dolaşımda olan Visa ve MasterCard temassız kredi kartlarında mikroişlemci ve anten gözükmezken, American Express kartında görünüyor.

Temassız Akıllı Kart Teknolojisi, RFID midir?

Gerek gazete, dergi köşe yazılarında gerekse bilimsel makalelerde, genellikle temassız kredi kartı teknolojileri, RFID olarak adlandırılan Radyo Frekanslı Tanıma sistemleri ile birlikte anılıyor ve önemli uygulama alanlarından biri olarak ele alınıyor. Temassız kredi kartlarında, pasif RFID teknolojisinde olduğu gibi çip üzerinde herhangi bir güç kaynağı yoktur. Kredi kartı, temassız kart okuyucu tarafından üretilen manyetik alana yaklaştırıldığında çip için gerekli enerji, anten üzerinden indüklenme yolu ile sağlanıyor (13,56 MHz radyo yayın frekansının 3 MHz-30 MHz arası yüksek frekans aralığında olması, kartın ana operasyon prensibinin manyetik olduğunu belirliyor) ve çip açık konuma geliyor. Bu noktadan sonra kablosuz iletişim protokolü başlıyor, çip ve okuyucu arasındaki veri transferi RFID teknolojisindeki gibi radyo yayını ile yapılıyor.

Tüm bu benzerliklerine karşın, temassız kredi kartı teknolojisinin RFID teknolojisinden farklı bir teknoloji altyapısına dayandığını söyleyenler (genellikle elektronik mühendisleri) bu farklılıkları şu şekilde dile getiriyor. Temassız akıllı kartlar, bilgi ve iletişim güvenliğinin önemli olduğu finans, bankacılık, hassas bilgi içeren e-devlet uygulamaları gibi alanlarda kullanılmak üzere ISO/IEC 14443 standardına uyumlu olarak tasarlanmıştır. Temassız kredi kartları bu tasarım nedeniyle 10 cm'den daha kısa mesafede etkileşime geçme ve iletişimini belli güvenlik protokollerine göre yapma kabiliyetindedir. RFID etiketlerinin sahip olmadığı güvenli bir şekilde veri depolama, veri erişimi, kriptografik protokolleri yerine getirme (AES, 3DES, RSA, ECC), karşılıklı tanıma özelliklerine sahiptir. Yani tasarımı diğer RFID okuyucular ile içindeki bilgilerin okunmasına izin vermiyor (http://www.smartcardalliance.org/pages/smart-cards-faq internet sitesinde oldukça ayrıntılı bir açıklama yer alıyor).

Aslında tüm bu ifadelerden de anlaşılacağı üzere temassız kartların RFID sistemlerle arasında tüm benzerliklere karşın temel bir fark var. Bu fark donanımsal açıdan üstünlüğe, güvenlik uygulamalarına ve 10 cm'den az aktivasyon alanına sahip olmasından kaynaklanıyor.

Bu nedenle eğer birisi çıkıp temassız akıllı kartlar eşittir "akıllı RFID" veya "ISO/IEC 14443 standardına uygun RFID" derse, o kişiye hatalı olduğunu söylemek doğru bir yaklaşım olmaz. Zaten hem bu yazıda kullandığımız hem de burada yer veremediğimiz başka bilimsel çalışmalarda, temassız akıllı kartların, RFID'nin alt kolu olduğuna yönelik bir kabul var. Özellikle kriptoloji ve bilgi güvenliğiyle uğraşanlar bu teknolojiyi yüksek güvenlikli RFID olarak görürken diğer uygulama alanlarındaki teknolojileri düşük maliyetli ve basit RFID olarak görüyor.

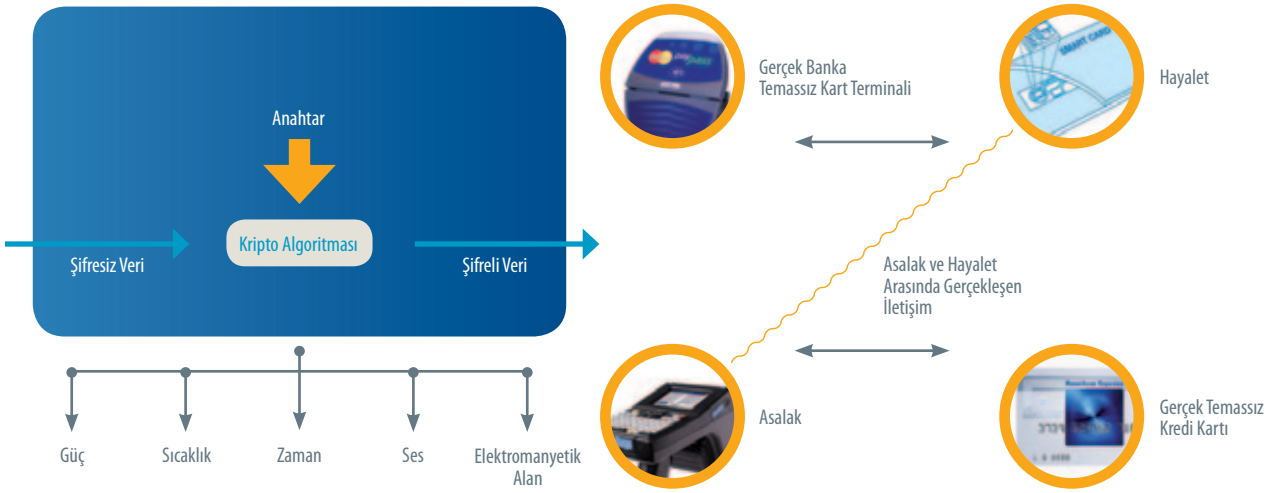
Temassız Kredi Kartları Güvenli mi?

İmza yok, kimlik göstermek yok, şifre girmek yok. İlk akla gelen risk de işte tam bu noktada başlıyor. Bu özellikleri ile nakit paradan farkı olmayan kartınızı kaybettiğinizi fark edene kadar hesaplarınızın boşaltılma riski var. Çip ve Şifre'li kartlarda ise, kart kaybedilse bile şifre bilinmediği için ilk etapta izinsiz kullanım imkânı da yok.

Kredi kartı şirketleri ve bankalar ise kullanılan bu teknolojinin çok güvenli olduğunu vurguluyor. Hatta kullanım sırasında kartlar sürekli kullanıcının kontrolünde olduğu için güvenlik derecesinin bir adım ileride olduğunu belirtiyorlar.

İnternette bu konu ile ilgili bir arama yaptığınızda karşınıza temassız kartlardaki güvenlik açıklarını gösteren onlarca sayfa çıkıyor ve endişe verici bir durum ortaya çıkıyor. Bu noktada internette yer alan bilgilerin bazen sansasyon yaratmak amaçlı olabildiği ve gerçek olmayabileceğini hatırlatmakta fayda var.

>>>

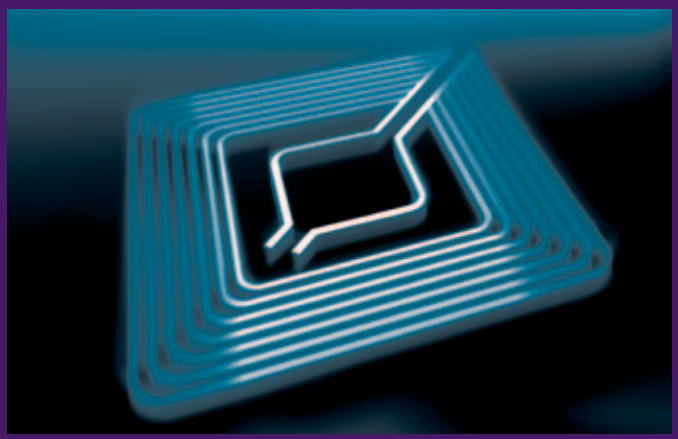


Yan Kanal Analizi: Temassız akıllı kartlar ve RFID sistemler gibi kablosuz iletişim teknolojilerine yönelik saldırılardan biri de Yan Kanal saldırılarıdır. Akıllı kart ve okuyucu arasında kablosuz iletişim gerçekleştirilirken veya akıllı kart üzerindeki çip, şifreleme ve şifre çözme işlemlerini yaparken güç, sıcaklık, zaman, ses ve elektromanyetik alan gibi bilgiler ortama verilmektedir. Bu bilgileri içeren sinyallerin yakalanması sonucu zaman, güç, sıcaklık gibi parametrelerdeki değişiklikler kripto anahtarı veya algoritması ile ilişkilendirilerek kriptografik varlık bilgileri elde edilmeye çalışılır. Eğer bu saldırı yöntemine karşı tasarım açısından gerekli karşı-güvenlik tedbirleri alınmazsa, kullanılan algoritma veya anahtar ne kadar güçlü olursa olsun ortama yayılan yan kanal bilgileri ile akıllı kart sistemi saldırılara açık hale gelebilmektedir.

Yeniden Yönlendirme Saldırısı: Bu saldırı çeşidinde anahtar veya şifreleme algoritmasının zayıflığından ziyade Yan Kanal saldırısındakine benzer şekilde temassız kartların fiziksel yapısından yararlanılmaktadır. Saldırgan amacına ulaşmak için iki araca ihtiyaç duyar. Bunlardan ilki, kurbanın taşıdığı temassız kredi kartı ile tıpkı bir banka POS cihazı gibi iletişim kuracak olan ve Asalak (*Leech*) olarak adlandırılan RFID okuyucusudur. İkincisi ise banka POS terminali ile iletişimi sağlayan ve kredi kartı gibi gözüken Hayalet (*Ghost*) adı verilen araçtır. Bu saldırı yönteminde Hayalet, gerçek banka POS terminali (okuyucu) ile tıpkı bir temassız kredi kartıymış gibi iletişim kurar ve POS'tan gelen istekleri Asalak'a iletir. Asalak da durumdan habersiz kurbana ait temassız kredi kartı ile iletişime geçer ve gerçek banka POS terminalinin isteğini akıllı karta iletir. Temassız karttan gelen cevap (onay) yine Asalak tarafından Hayalet'e iletilir, Hayalet gerçek bir banka kartıymış gibi onayı POS cihazına iletir ve ödeme işlemi tamamlanmış olur.

Temassız akıllı kart özelliğine sahip kredi kartları ve e-pasaportlarda, kartın çalışma şeklinden kaynaklanan, radyo yayını yaparken saldırılara açık hale gelme tehlikesini en azından aktif kullanım dışındaki zamanlarda engellemek için, Faraday kafesi etkisine sahip birtakım ürünler de (kılıf, cüzdan gibi) şık tasarımları ile raflardaki yerlerini almaya başladı.

Temassız Akıllı Kartlar ve Güvenlik Açıkları



Kredi kartı şirketlerinin kartların yüksek kriptoloji ile korunduğunu belirtmiş olmasına karşın, temassız kredi kartlarının ilk nesil ürünleri ile ilgili ciddi güvenlik açıkları olduğu, 2006 yılında Kevin Fu liderliğindeki Massachusetts Üniversitesi araştırmacıları ve ABD merkezli RSA şirketi tarafından yapılan bir çalışma ile gösterildi. Bu çalışmada araştırmacılar ABD'de faaliyet gösteren üç büyük kredi kartı şirketine ait, değişik bankalar tarafından kullanılmakta olan 20 adet RFID özellikli temassız kredi kartını inceledi. Bir bilgisayar ve yaklaşık 150 dolara mal edilen ev yapımı ekipman ile araştırmacılar bu kartlardan bir tanesini tamamen kopyalayabildiler ve bu kartın Tekrarlama Saldırısı'na (*Replay Attack*) açık olduğunu ve alışverişlerde kullanılacak hale getirilebildiğini gösterdiler. Özetle ifade edecek olursak, Tekrarlama Saldırılarında RF okuyucu tarafından gönderilen sorguya temassız kart tarafından verilen cevap sinyali yakalanıyor ve daha sonraki bir seansta bu mesajın aynısı kullanılarak saldırı gerçekleştirilebiliyor. Bu araştırmada elde edilen en ilginç ve önemli bulgulardan biri de test edilen kartların büyük bölümünün kullanıcı adını, kredi kartı numarasını ve kartın geçerlilik süresini şifresiz bir şekilde yayımladığının tespit edilmesi oldu. Neyse ki, kartların arka yüzlerinde bulunan üç haneli güvenlik kodu bilgisine ulaşılamamış. Bu nedenle internet üzerinden alışverişlerde kullanımı kısıtlı olsa bile, bu kodu sormadan alışveriş imkânı sağlayan alışveriş siteleri var. Bahsedilen ilk nesil temassız kartlardaki güvenlik açıkları işin sadece bir yönü. Dr. Kevin Fu ve arkadaşları buradaki temel problemin sadece güvenlik açıkları değil, gizli kalması gereken kişisel bilgilerin açık edilmesi olduğunu belirtiyor.

Bahsedilen bu güvenlik açıkları ilk nesil temassız kartlarda vardı. Yapılan bu bilimsel çalışmadan sonra kredi kartı şirketleri (Visa, MasterCard, Amerikan Express) bankaların kredi kartı üzerindeki ismi yayımlamasını engelledi.

Endişelenmeli miyiz?

Temassız kartların en büyük zafiyeti (eğer gerekli önlemler alınmazsa) herhangi bir radyo frekans iletimine karşılık verme özellikleri. Buna kablosuz yayın yapma özelliği de eklenince, kişisel bilgilerin gittiği yerler üzerinde kart sahibinin kontrol yetkisi doğal olarak azalmış oluyor. Durum böyle olmasına rağmen, bildiğimiz kadarıyla şu ana kadar kayıt altına alınmış bir sahtekârlık olayı yok ve bahsedilen güvenlik açıkları da sadece laboratuvar ortamında ve belli bir bilgi birikimine sahip kimseler tarafından gösterildi.

Diğer taraftan, yüzlerce milyar dolarlık bir endüstri haline gelen kredi kartı pazarında, servis sağlayıcı şirketler de boş durmuyor ve en son teknolojili güvenlik uygulamalarını hayata geçiriyorlar. Yazıda bahsettiğimiz bilimsel çalışmalarda anlatılan saldırıların birçoğuna karşı önlemler de literatürdeki diğer çalışmalar ile verilmektedir. Her geçen gün, açıklar ortaya çıktıkça önlemler alınıyor ve sistemler giderek daha güvenli bir hal alıyor. Bankalar kredi kartları ile yapılan alışverişlerde şüpheli durumları fark edebilmek için özel olarak geliştirilmiş yazılımlar da (*antifraud systems*) kullanıyorlar. Örnek olarak, Ankara'da bir alışveriş yapıldıktan sonra yarım saat içinde İstanbul'da bir alışveriş yapılırsa, mevcut yazılım bunu algılayıp şüpheli bir durum olduğunu yetkililere bildiriyor.

Diğer yönden bankalar arası farklı uygulamalar da olabiliyor. Konuyu biraz daha açarsak, kredi kartı üzerindeki güvenlik özelliklerinin maliyet ve işlem süreleri üzerindeki etkisini ve olası dolandırıcılık tehditlerini göz önüne alarak, her banka politikaları doğrultusunda kendi güvenlik seviyesini belirliyor. Örnek olarak yüksek seviyeli kriptoloji kullanmanın işlem süresini uzatıcı etkisi olduğundan bu yöntem (ABD'deki ve Avrupa'daki) bazı bankalar tarafından tercih edilmeyebiliyor.

Yeni teknolojilerin kullanım açısından büyük kolaylık sağlıyor olması ve gelişmiş ülkelerde de bu tür uygulamaların yaygın olması, ülkemiz açısından bu ürünlerin güvenli olduğu anlamına gelmiyor. Birçok konuda olduğu gibi bankacılık alanında da farklı uygulamalar var. Örneğin ABD gibi gelişmiş ülkelerde kredi kartı sahtekârlıklarında mağdur olan kişinin beyanatı yeterli görülüp sigorta devreye girebiliyorken, maalesef ülkemizde bu mağduriyetlerin belgelendirilmesi istenebiliyor.

Şimdilik internetten yapılan alışverişlerde maruz kalınan sahtekârlıklar (*phishing* ve *keylogger* saldırıları gibi) ve ATM cihazları üzerinden yapılan diğer saldırılar daha etkin görünüyor ve temassız kart teknolojisinde yapılacak sahtekârlıklar diğerlerine nazaran daha fazla çaba gerektiriyor. Bu nedenle temassız kartlar şimdiye kadar kötü niyetli kişilerin ve sahtekârların dikkatini çekmemiş gibi görünüyor. Diğer yandan, kredi kartı pazarının giderek büyümesi ve kullanılmakta olan sistemlerin gün geçtikçe daha güvenli hale gelmesi (internet bankacılığında tek kullanımlık şifrenin zorunlu hale getirilmesi, kredi kartlarında şifre uygulamasına geçilmesi, vs.) gibi sebeplerden ötürü ye-

Temassız akıllı kartlara yönelik tehlikeli saldırı yöntemlerinden biri de Yeniden Yönlendirme saldırılarıdır (*Relay Attack*). Bu yöntemde amaçlanan aktarılan şifreli verilerin çözülmesi değil, gerçek kredi kartı ile gerçek banka POS cihazı arasında kurbandan habersiz olarak aracılık edilip, ödemenin kurbanın kredi kartı üzerinden yapılmasıdır. Gerhard Hancke gerçekleştirdiği bilimsel bir çalışmada ISO 14443A standardına uygun olan temassız akıllı kartların Yeniden Yönlendirme saldırısına açık olduğunu ve Asalak ile Hayalet arasındaki mesafenin 50 metreyi bulabildiğini göstermiştir. Bir başka çalışmada Kifr ve Wool çok daha ciddi sonuçları olabilecek bir saldırı gerçekleştirdiler. Temassız akıllı kartların en önemli güvenlik önlemi 10 cm ve daha az bir mesafeden aktif hale gelmeleri ve okunabilmeleridir. Kifr ve Wool gerçekleştirdikleri Yeniden Yönlendirme saldırısında, pasif akıllı kartın aksine aktif Hayalet kullanıp Banka POS cihazının aktivasyon alanı içinde (10 cm) olma zorunluluğunu kaldırmışlar ve bu mesafeyi 50 metreye kadar çıkarmışlardır. Ayrıca kendi yaptıkları Asalak görevi gören ekipmanın, kurbanın kredi kartından 50 cm uzaklığa kadar etkin olabildiğini göstermişlerdir. Bu ise, Asalak ile Hayalet arasındaki etkin iletişim mesafesine göre kurbanın kredi kartından oldukça uzak bir noktadaki ödeme noktasından saldırı yapılabileceğini göstermektedir.

Diğer taraftan bu tür Hayalet-Asalak saldırılarına karşın araştırmacılar da boş durmuyor ve birtakım Mesafe Sınırlama Protokolleri geliştiriyorlar. Örneğin temassız akıllı kart gerçekten meşru bir okuyucu yakınındaysa (belirli bir mesafe içindeyse) belirli bir delta süresi içinde çeşitli sorgulamalara cevap vermesi gerekir. Sorgu cevaplama işleminde sinyal geliş gidiş zamanına göre, okuyucu ile temassız akıllı kart arasındaki mesafenin üst limiti, ışık hızı baz alınarak hesaplanabilir (hiçbir şey ışıktan daha hızlı hareket edemeyeceği için). Ancak Asalak ve Hayalet devrede olduğu zaman bu süre belirlenmiş delta zamanını aşacağından saldırı fark edilip bertaraf edilebiliyor.

Ulaşım Sektöründe Kullanılan Kartlar

MIFARE Classic, dolaşımda olan bir milyardan fazla temassız kartı ile şu an dünyada %70'lik oran ile en yaygın kullanılan sistem. Özellikle Hong Kong'ta Octopus Card, Londra'da Oyster Card ve diğer metropoller gibi yüksek yoğunlukta çalışan toplu taşıma bilet sistemlerinde ve Asya ülkelerindeki bazı finans kuruluşlarında kullanılıyor. Dolaşımda bu kadar çok temassız akıllı kart olunca ister istemez güvenlik endişeleri de doğuyor. Son yıllarda bilim insanları ve araştırmacılar, MIFARE teknolojisinin güvenlik açıklarına dair çalışmalar yapıyor. Gerhard de Koning Gans ve diğer araştırmacıların 2008 yılında uluslararası bir konferansta sonuçlarını sunduğu çalışma, MIFARE Classic teknolojisine yönelik düşük maliyetli, pratik bir saldırı neticesinde bellek içindeki gizli bilgilerin açık edilebileceğini gösterdi. Benzer bir başka çalışmada F. D. Garcia ve diğer araştırmacılar (2009), uygulanan çeşitli saldırı senaryolarının birinde, mevcut açık nedeniyle 1 saniyeden daha az bir sürede gizli anahtarın bulunabildiğini, ayrıca akıllı karta kablosuz erişim olduğu zaman akıllı kartın Yan Kanal (*Side Channel*) saldırılarına da açık olduğunu gösterdiler.

Önümüzdeki aylarda Yakın Saha İletişimi (NFC) teknolojisi sayesinde cep telefonları artık birer temassız kredi kartı gibi kullanılabilecek. Ülkemizde faaliyet gösteren bazı GSM operatörleri ve bankaların ortaklaşa gerçekleştirdiği bir proje ile SIM kartlara kredi kartı özelliği kazandırılacak. Bu sayede NFC uyumlu cep telefonu alma zorunluluğu olmadan, yeni bir SIM kart alarak telefonlarınızla temassız ödeme noktalarında alışveriş yapabileceksiniz.

ni bir pazar olan temassız kart teknolojisi, yakın bir gelecekte sahtekârlıklar açısından daha fazla ilgi çekecek gibi.

Sonuç olarak bu kartlar, günlük hayatın koşuşturması ve karmaşası içinde getirdikleri kolaylık ve hız ile hayatımızda daha çok yer edecek gibi görünüyor. Sunulan bilgiler ve deliller ışığında, hem yeni nesil kartların güvenlik özellikleri hem de saldırganların ilgisini henüz tam olarak çekmemiş olması nedeniyle şimdilik çok büyük bir risk gözükmüyor. Görünen en büyük risk, kullanıcının kartını kaybetmesi. Buna karşı alınabilecek en iyi önlem kartların güvenli bir şekilde saklanması ve düzenli aralarla kartlardan herhangi birinin kaybolup kaybolmadığının kontrol edilmesi.

Kaynaklar

Heydt-Benjamin, T. S., Bailey, D. V., Fu, K., Juels, A., O'Hare, T., "Vulnerabilities in First-Generation RFID-enabled Credit Cards", http://www.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf

Gans, G. K. , Hoepman, J. , Garcia, F. D. , "A Practical Attack on the MIFARE Classic", *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*, s. 267-282, 08-11 Eylül, 2008.

Garcia, F. D., Rossum, P. V. , Verdult, R., Schreur, R. W., "Wirelessly Pickpocketing a Mifare Classic Card", *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, s. 3-15, 17-20 Mayıs, 2009.

Hancke, G. P., "A Practical Relay Attack on ISO 14 443 Proximity Cards", Manuscript. [Online]. Available: http://www.rfidblog.org.uk/hancke-rfidrelay.pdf

Kfir, Z. , Wool, A., "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard", *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (SECURECOMM'05), s.47-58, 05-09 Eylül, 2005.

"Researchers See Privacy Pitfalls in No-Swipe Credit Cards", http://www.nytimes.com/2006/10/23/business/23card.html?pagewanted=2

www.rfidjournal.com