TEMASSIZ AKILLI KARTLARA PRATİK BİR SALDIRI

Oğuzhan Urhan

Elektronik ve Haberleşme Mühendisliği Bölümü
Kocaeli Üniversitesi
urhano@kou.edu.tr

ÖZET

Bu yazıda, ISO14443 protokolüne göre çalışan temassız akıllı kartlara (contactless smart card) yapılan yeniden yeniden yönlendirme saldırısı (relay attack) hakkında bilgi verilecektir. Bu saldırıda, şifreleme yöntemlerinin bir açığına veya şifreleme kullanılan anahtarların (key) bilinmesine gereksinim duyulmamaktadır. Sistemdeki açık tamamı ile verinin kablosuz olarak aktarılması nedeni ile yani fiziksel nedenlerden kaynaklanmaktadır.

1. GİRİŞ

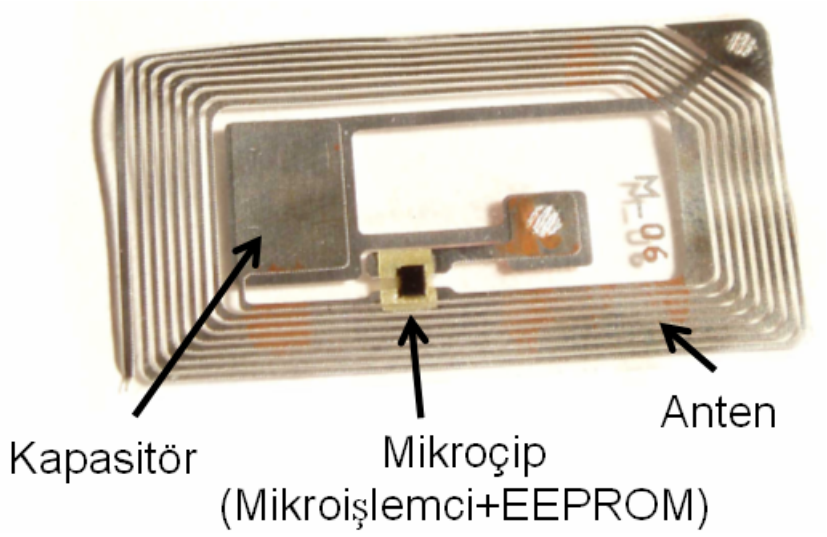
Bilimin önemli amaçlarından biri geliştirdiği teknoloji ile insan yaşamını kolaylaştırmaktadır. Erişim kontrolünün ve para kullanımının elektronik olarak gerçekleştirilmesi hayatımızı kolaylaştıran önemli bazı uygulamalardır. Günlük yaşamımızda sıkça kullanmak durumunda olduğumuz paranın elektronik ortamda saklanması fikri yine yaşamımızı kolaylaştırmak hedefi ile ortaya çıkmıştır. Ancak paranın elektronik ortamda saklanması beraberinde bazı güvenlik sorunlarını da beraberinde getirmektedir. Çünkü yeterli güvenlik önlemlerinin alınmaması durumunda paranın elektronik olarak kopyalanması kalpazanlık yoluyla fiziksel olarak kopyalanmasından daha kolaydır. Erişim kontrolü uygulamalarında ise şirketler personellerine dağıttıkları elektronik kimlikler ile sadece izinleri bulunan kısımlara giriş yapmalarına olanak sağlamaktadırlar. Bu gibi bir elektronik kontrol sistemi ile geçiş noktalarından hangi zamanda kimlerin geçtiği de kolaylıkla izlenebilmektedir.

Yukarıda sayılan uygulamalar için genellikle akıllı kartlar (smart card) ve iButton adı verilen donanımlar kullanılmaktadır. Akıllı kartların temel olarak temaslı, temassız (contactless) ve karma (hybrid) olmak üzere üç tipi bulunmaktadır. Temaslı akıllı kartlarla geçişin sağlanabilmesi veya para yükleme/düşme işleminin yapılabilmesi için kart ile okuyucu donanım (terminal) arasında fiziksel bir teması gerekmektedir. Böylelikle akıllı kart çalışması için gerekli olan elektrik enerjisini terminal üzerinden sağlar ve veri iletişimi fiziksel temas ile elektriksel olarak sağlanır. Temassız akıllı kartlar ise terminalle haberleşme için fiziksel temasa gereksinim duymazlar. Okuyucu terminale belirli bir miktar yaklaştırılmaları durumunda enerji ve veri aktarımı kablosuz olarak elektromanyetik dalgalar vasıtası gerçekleştir. Temassız kartların 10cm ve altı gibi yakın mesafede çalışan (proximity card) ve 1 metreye kadar uzak mesafede (vicinity card) çalışan tipleri mevcuttur. Para söz konusu olduğu zaman genellikle yakın mesafede çalışan temassız akıllı kartlar kullanılırken, erişim kontrolü uygulamalarında hem uzam hem de yakın mesafede çalışan temassız akıllı kartlar kullanılabilir. Karma tipteki akıllı kartlarda ise terminalle haberleşme için hem temaslı arayüz hem de temassız arayüz bulunmaktadır. iButton'larda kullanılan uygulamalarda ise iButton'u terminale dokundurmak yeterlidir. iButton kullanımına en yaygın örnek olarak İstanbul'da kullanılan AKBİL sistemi verilebilir.

2. TEMASSIZ AKILLI KARTLARA YENİDEN YÖNLEDİRME SALDIRISI

Temassız akıllı kartlar son yıllarda yaygın olarak birçok uygulamada kullanılmaya başlanmıştır. Türkiye'de ise en yaygın kullanımı 2 milyon kişi ile İzmir'de kullanılan "Kent Kart" sistemindir. Ön ödemeli taşımacılık için kullanılan bu sistem, yakın zamanda Manisa (2004) ve Denizli (2005) belediyeleri de bu sistemi taşımacılık sektöründe kullanmaya başlamışlardır [1]. Bu sistemi Türkiye'de kullanıma alan Kent Kart Ege Elektronik San. Tic. Ltd. Şti, adlı firma Philips firması tarafından geliştirilen Mifare adı verilen kartları kullanmaktadır [2,3]. Firma, 2000 yılında akıllı kart ile gerçekleştirilen en iyi taşımacılık dalında Sesame 2000 ödülünü almıştır [3]. "Kent Kart" sisteminde kullanılan temassız kartlar ISO14443 protokolüne göre çalışmaktadır [4]. Sadece Mifare değil temassız olarak çalışan birçok akıllı kart ISO14443 protokolüne göre çalışmaktadır.

Temassız akıllı kartlar aslında içerisinde mikroişlemci, haberleşme için anten ve gerekli gücü terminalden almak için kapasiteden oluşmaktadır (Bkz. Şekil-1). Temassız akıllı kart içerisindeki mikroişlemcinin çalışabilmesi için enerjiye gereksinimi bulunmaktadır. Bu enerji ise, kart okuyucu terminal tarafından aktarılan aktarılmakta ve kart üzerindeki anten vasıtası ile toplanıp kapasitörde depolanıp kullanılmaktadır. ISO14443 protokolüne göre yakın mesafede çalışan (proximity) temassız kartlar ile terminal arasındaki haberleşme arasındaki haberleşme 13.56MHz'de gerçekleştirilmektedir. Terminal ile kart arası mesafenin 0-10cm arası olması gerekeli güç aktarımı için yeterlidir



Şekil-1 Temassız bir kartın iç yapısı [5]

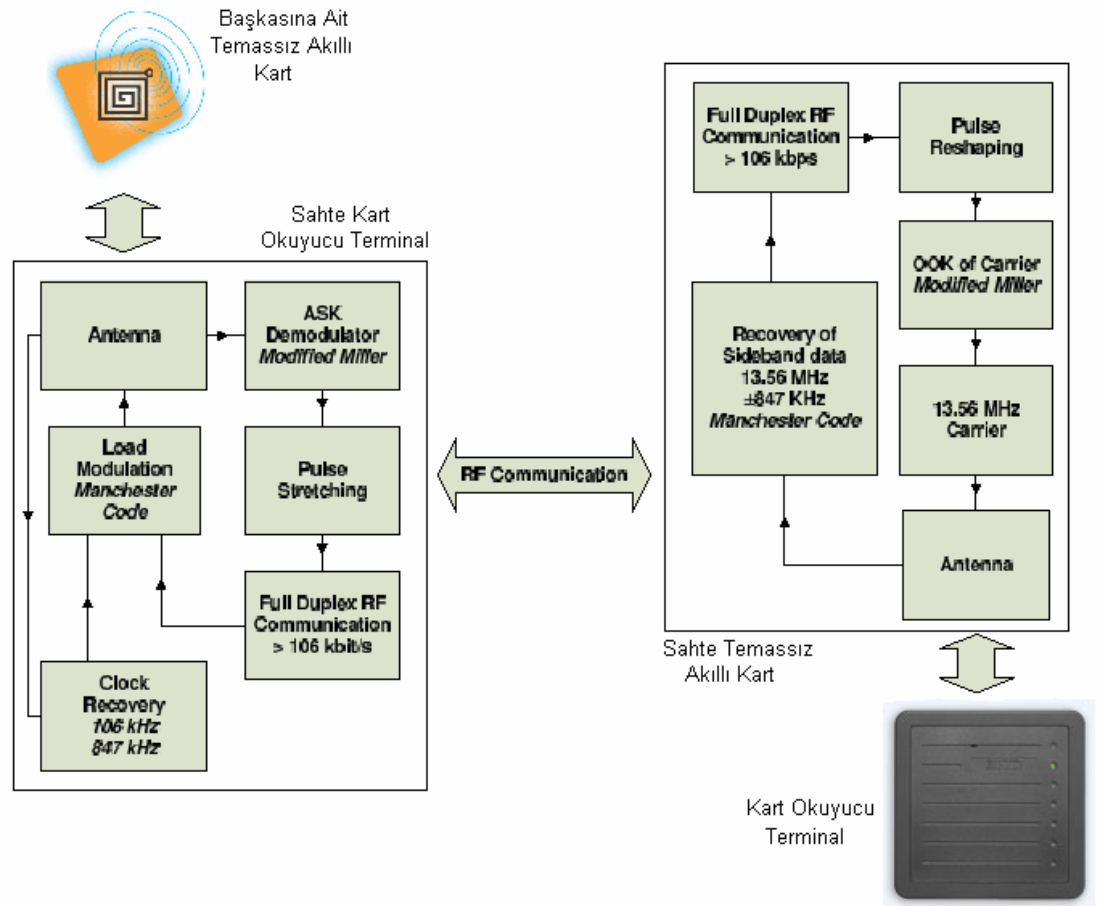
Mikroişlemci ile kart okuyucu terminal arasında şifreli bir haberleşme gerçekleştirilerek kontör veya para yükleme ve düşme işlemleri gerçekleştirilmektedir. Bu aşamada kullanılan 3-DES, RSA gibi güçlü şifreleme algoritmaları ile aktarılan verinin güvenliği sağlanmaktadır. Doğrudan şifreleme sistemine yapılacak saldırılar ile sistemin güvenliğinin tehlikeye sokulması çok mümkün görünmemektedir. Bu tip sistemlere saldırılar genellikle farksal güç analizi (Differential Power Attack-DPA) veya basit güç analizi (Simple Power Analysis-SPD) yöntemleri ile yapılmakta ve akıllı kartla gerçekleştirilen iletişim sırasında harcanın güç analiz edilerek gizli anahtarlar (secret keys) ortaya çıkarılmaya çalışılmaktadır [6].

Ayrıca akıllı kartlar bazı fiziksel saldırılara karşı dayanıksız olduğu iddia edilmektedir. Örneğin EEPROM'da saklanan bilginin ultraviyole ışık ile silinebileceği veya kart içerisinden

sökülen mikroişlemci üzerinden çeşitli verilerin microprobing yöntemi ile çekilmesi mümkün olduğu ileri sürülmektedir [7-8]. Ancak bu işlemler özel laboratuvar koşullarında gerçekleştirilebileceğinden pratik saldırılar olarak değerlendirilmeyebilir.

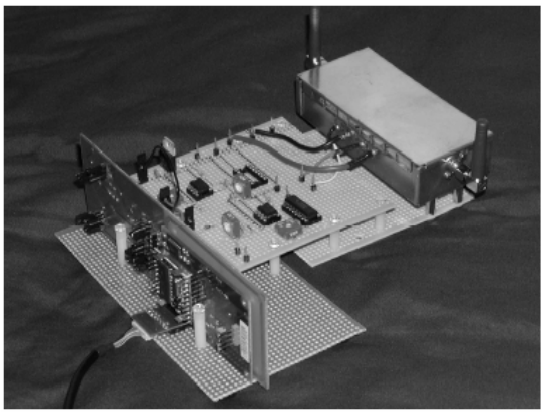
2005 yılının başlarında ISO14443 protokolünü kullanan temassız kartlara karşı yeni bir saldırı geliştirilmiştir. Bu saldırıya tekrar yönlendirme saldırısı (relay attack) adı verilmektedir [9,10]. Bu saldırıda amaçlanan başkasına ait bir kartı geçiş noktasında kart sahibinin haberi olmadan kullanmaktadır. Yeniden yönlendirme saldırısında temel olarak saldırıyı gerçekleştiren kişi, terminal ile akıllı kartmış gibi haberleşirken (konuşurken), akıllı kartla terminalmiş gibi haberleşmektedir. Bu saldırıda temassız akıllı kartların veri iletişimine geçmesi için gerekli enerjiyi terminalden almasından yararlanılmaktadır. Normalde terminal ile kart arası mesafenin 0-10cm olması yeterlidir. Ancak daha güçlü antenler kullanılarak bu kartlar daha uzak mesafelerden de kullanılabilmektedir.

Cambridge Üniversitesi'nden Gerhard Hancke yaklaşık 200$'a mal olan basit bir sistem ile para ödeme noktasından geçerken yakında bulunan başkasına ait bir temassız akıllı kartın kullanabilmesine imkan sağlayan bir saldırı pratik olarak gerçeklenmiştir [9]. Aynı saldırı Tel Aviv Üniversitesi'nden bir grup tarafından da gerçekleştirilmiştir [10]. Bu düşük maliyetli sistemde kullanılan elektronik donanım ile kart okuyucuya, bir kartmış gibi davranılıp haberleşilirken, başkasına ait akıllı kart ile de terminalmiş gibi haberleşilmektedir. Burada aktarılan verinin çözülmesi gibi amaç güdülmemektedir. Sadece örneğin kontör düşme noktasında (örneğin otobüse/metroya binerken) başkasına ait bir kart ile haberleşilerek para o kart üzerinden ödetilmektedir. Bu durumun kartı habersiz olarak kullanılan kişinin o anda haberdar olması mümkün değildir.

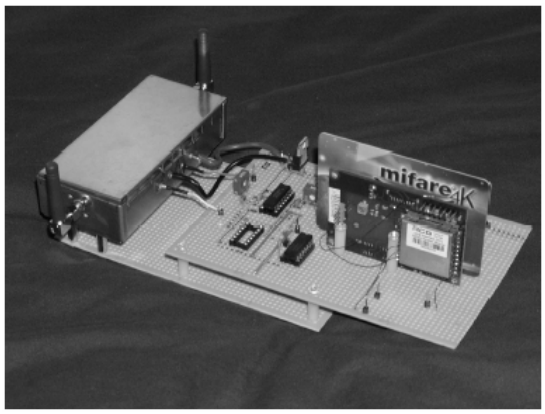


Şekil-2 ISO 14443 protokolünü kullanan kartlara yapılan tekrar yönlendirme saldırısı [9]

Yakın mesafede çalışan temassız kartlar (proximity) normalde terminale 0-10cm arası yakınlaştırıldıklarında devreye girer ve sonrasında kontör/para düşme işlemi gerçekleşir. Bu sistem kullanılan düşük maliyetli elektronik donanım ile bu mesafe artırılmakta ve 50cm civarda bulunan herhangi bir temassız akıllı kart sahibinden habersiz olarak kullanılabilmektedir. Mesafenin artırmak için antenin fiziksel büyüklüğü, kalite faktörüne (Q factor) ve aktarılan güce bağlıdır [9,10]. 13.56MHz'lik haberleşme frekansı için en uzak haberleşme mesafesi 3.5m'yi bulmaktadır [10]. Bunu pratikte gerçekleştirmek için antenden geçen akımın artırılarak oluşturulan manyetik alanının şiddetinin artırılması veya antenin gerekmektedir. Ancak antenden geçirilen akımın artırılması durumunda oluşan dahili gürültü akıllı karttan zayıf işaretin daha da düşmesine neden olabilir. Ayrıca anten boyutunun büyütülmesi, dışarıdan daha fazla gürültü alınmasına ve yine akıllı karttan alının işaret seviyesinin düşmesine neden olabilir [10]. Böyle bir saldırıda kullanılacak sistemin taşınabilir (mobil) olması için anten boyutunun fazla büyütülmesi zaten pek mümkün değildir. Bu kısıtlamalar nedeni ile sahte kart okuyucu terminal ile saldırıya uğrayacak kart arasında mesafenin pratikte 50cm'den daha uzak olması mümkün görünmemektedir. Şekil-2 ve Şekil-3'de Cambidge Üniversitesi'nde bu amaçla gerçekleştirilen prototip sistemin blok şeması ve donanımsal yapısı görülmektedir.



Sahte temassız akıllı kart



Sahte kart okuyucu terminal

Şekil-3 ISO 14443 protokolüne göre haberleşen kartlardaki açığı kullanmak için geliştirilen prototip [8]

Burada önemli olan diğer bir nokta temassız akıllı kart görevini yerine getiren donanım ile kart okuyucu terminal görevini gören donanımın birbirine yakın olması gerekmemesidir. Örneğin saldırıyı gerçekleştirmek isteyen iki kişilik bir ekipten bir kişi (sahne okuyucu terminal görevini yerine getiren) durakta otobüs bekleyen kişilerin yanına 50cm kadar yaklaşabilir. Bu sırada diğer kişi otobüse binerken sadece saldırıyı gerçekleştiren diğer kişideki donanımla haberleşmek zorundadır. Bu mesafe ise yüzlerce metre olabilir. Dolayısıyla saldırıyı sadece 50cm mesafe içerisinde yapılabilir kabul etmek doğru bir yaklaşım olmayacaktır.

Bu prototip daha uygun antenler kullanılıp, baskılı devre üzerine aktarıldığında çok daha küçük bir alan kaplayacak (küçük bir evrak çantası kadar) ve pratik olarak kullanılabilecektir. Bu saldırıya karşı şu ana kadar geliştirilmiş geçerli bir koruma yöntemi bulunmamaktadır. Çünkü sorun şifreleme yöntemlerinden kaynaklanmamakta kartın fiziksel yapısı ve çalışma şeklinden ortaya çıkmaktadır. Kart kullanıcılarının yapabileceği kartlarını Faraday kafesi etkisi yapacak bir ortamda (kılıf) saklayarak, sadece kullanmak istediklerini bu kılıftan çıkarıp kullanmalarıdır.

Bu gibi bir saldırıyı engellemek için Kent Kart sisteminde basit ama pek işlevsel olmayan bir koruma bulunmaktadır. Bu basit korumada bir kartın yarım saat içerisinde aynı validatörden (kart okuyucu) iki kez ödeme yapması önlenmektedir. Aynı kartın yarım saat içerisinde iki kez ödeme yapması için bir görevlinin buna onay vermesi gerekmektedir. Ancak bu gibi bir koruma sistemin esnekliğini azaltmaktadır ve sistemin tam otomatik çalışmasının önünde bir engel olarak durmaktadır. Ayrıca bu önlemin tam bir koruma sağladığı da söylenemez. Çünkü daha önce açıklandığı gibi akıllı kart yerine geçen donanımla, terminal yerine geçen donanınım arasındaki mesafe yüzlerce metre olabilir. Dolayısıyla saldırıya uğrayan (ve bundan hiçbir şekilde haberi olmayan ve saldırı esnasında haberi olamayacak) kişinin parası otobüse/metroya binmese bile başkası tarafından kullanılabilir.

Bu saldırı sistem sahibi/yöneticisi (örneğin belediye) açısından mali bir kayba neden olmamakla birlikte kullanıcıların parasının bir anlamda çalınmasına neden olmaktadır. Bu da kullanıcıların sisteme güveni zedeleyecektir ve bu elektronik cüzdan uygulamaları için kabul edilebilir değildir.

3. SONUÇ

Bu yazıda ISO14443 protokolüne göre haberleşen temassız akıllı kartlara pratik olarak uygulanabilecek yeniden yönlendirme saldırısı hakkında bilgi verilmiştir. Saldırı, şifreleme sisteminin bir açığından değil de temassız kartların fiziksel yapısından kaynaklandığından saldırının tamamı ile önlenmesi olası görünmemektedir. Saldırı oldukça düşük maliyetli bir donanımla gerçekleştirilebileceğinden (200$ civarı) ve tespitinin neredeyse imkansız olması nedeni ile oldukça etkilidir. Bu tip kartları kullanan sistemler tarafından alınabilecek pek fazla önlem olmamakla birlikte, kullanıcılar kartlarını Faraday kafesi etkisi yapacak kılıflarda saklayarak kendilerini koruyabilirler.

KAYNAKLAR

1. http://www.kentkart.com.tr (6 Aralık 2005)
2. http://www.mifare.net/products/company.asp?Company=349 (6 Aralık 2005)
3. http://www.semiconductors.philips.com/acrobat_download/literature/9397/75015156.pdf (6 Aralık 2005)
4. http://www.mifare.net/about/standards.asp (6 Aralık 2005)
5. Jonathan Westhues, "A Practical Attack on a Proximity Card" http://www.recon.cx/recon2005/papers/Jonathan_Westhues/montreal-pres.ppt (6 Aralık 2005)
6. Robert Sloan, "Smart-Card Security under the Threat of Power Analysis Attacks" www.ccs.uky.edu/ccs/Mar03.ppt (5 Aralık 2005)
7. http://www.cypherpunks.to/~peter/T7_Smart_Cards.pdf (5 Aralık 2005)
8. http://people.cs.uchicago.edu/~dinoj/smartcard/security.html (5 Aralık 2005)
9. Gerhard Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards" http://www.cl.cam.ac.uk/~gh275/relay.pdf (5 Aralık 2005)
10. Ziv Kfir, Avishai Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems," Cryptology ePrint Archive, Report 2005/052, http://eprint.iacr.org/2005/052.pdf (5 Aralık 2005)