Mobil Ödemeler, Güvenlik Sorunları ve Çözüm Önerileri

Barış İŞLER*
Hakan GÜLAÇ**

Özet

Gelişen bilgi teknolojileri ve hızlanan bilgi sistemleri altyapıları ile birlikte, mobil ödeme sistemi kullanımı ve bununla birlikte güvenlik riskleri de artmakta ve mobil ödemelerde yoğun kişisel ve finansal veri kullanılması nedeniyle saldırganların ilgisini çekmektedir. Bu çalışmada, ödeme verisinin ekstra güvenlik katmanıyla korunması, ödeme teyidinin hassas ödeme verisi yerine farklı bir dinamik unsurla yapılması gerektiği sonucuna ulaşılmıştır. Ayrıca, NFC ödemelerde cihazların pasif modda çalıştırılması, POS cihazı ile arasındaki haberleşme süresine kısıt konulması, NFC ödemeler için kullanıcı farkındalığının artırılması, QR kodlu ödemelerde, her ödemede değişken bir kod kullanılması, URL yönlendirilmesinin işyeri tarafından yapılması ve domain adının kısa olması önerilmektedir.

Anahtar Kelimeler: *Mobil Ödeme, NFC, QR Kodu, USSD/SMS, Sosyal Medya*

JEL Sınıflandırması: *G21, G23, O33, O35*

Abstract - Mobile Payments, Security Issues and Solutions

Along with the developing information technologies and accelerated information systems infrastructure, the use of mobile payment systems, as well as security risks, increase and attract the attention of attackers due to the use of intensive personal and financial data in mobile payments. In this study, it is concluded that the payment data should be protected with an extra security layer and the payment confirmation should be done with a different dynamic element instead of the sensitive payment data. Furthermore, it is recommended that NFC device should be run in passive mode, limiting communication time between NFC device and POS device, increasing user awareness for NFC payments and at QR code payments, variable code at each payment, URL redirection by the merchant and short domain name should be used.

Keywords: *Mobile Payment, NFC, QR Code, USSD/SMS, Social Media*

JEL Classification: *G21, G23, O33, O35*

* Bankacılık Başuzmanı, Bankacılık Düzenleme ve Denetleme Kurumu
** Dr, Grup Başkanı, Sermaye Piyasası Kurulu

1. Giriş

Mobil ödeme "mallar, hizmetler ve faturaların kablosuz iletişim teknolojileri yardımıyla mobil cihazlar vasıtasıyla gerçekleştirilmesi" olarak tanımlanmaktadır (Dahlberg, Mallat, v.d., 2008). Mobil ödemeler, işyerlerine; kullanıcıların konumu, alışveriş alışkanlıkları ve alışveriş tercihleri bilgilerini kullanarak, kullanıcılara daha kişiye özel ve kaliteli hizmet verme imkânını sunmaktadır. İşyerleri böylece, bütün kullanıcıları kapsayan küçük fırsatlar yerine doğrudan hedef kitleye yönelik daha avantajlı kampanyalar gerçekleştirerek yeni müşteriler kazanabilmektedir. Kullanıcılara ise kartla alışverişe göre daha kullanışlı ve hızlı ödeme hizmetinin yanı sıra, ürünlerin farklı yerlerdeki fiyatına, indirimlere ve diğer kampanyalara ait bilgiye erişim ve kıyaslama kolaylığı sunmaktadır. Ayrıca hareketliliğin artmasıyla mobil ödeme sistemleri kredi kartı ve nakit gibi ödeme araçlarına önemli bir alternatif haline gelmektedir (Ondrus ve Pigneur, 2006). Buna ek olarak, gelişmekte olan ülkelerde banka hesabı olmayan insanların dahi mobil telefona sahip olduğu gerçeği, mobil telefonların gerek bilgi verme gerekse işlem yapma amaçlı finansal hizmetlerin sunulabilmesi yönünde ciddi bir potansiyel sunmasına neden olmaktadır (TBB, 2011).

2015 yılında ISACA (Information Systems Audit and Control Association/Bilgi Sistemleri Denetim ve Kontrol Birliği) tarafından gerçekleştirilen Mobil Ödemelerde Güvenlik Çalışmasına göre, 2020 yılına kadar mobil ödeme piyasasının pazar büyüklüğünün 2,8 trilyon dolar olacağı belirtilmektedir.

Kartlı sistemler yıllardan beri gelişen bir güvenlik altyapısına sahip olduğundan dolayı aksini belirten birkaç görüşe rağmen (Murdoch, Drimer, v.d., 2010) kabul edilebilir güvenlik sunmaktadır. Buna karşılık iletimde hava ortamını kullanması, mobil cihazların kolaylıkla ele geçirilebilir ve tekrar kullanılabilir olması ve mobil işletim sistemlerinin güvenlik unsurlarının kısıtlı olması, mobil sistemleri dolandırıcılığa daha fazla müsait hale getirmektedir. Dolayısıyla, mobil ödeme sistemlerinde güvenlik üzerinde daha fazla durulması gerekmektedir. Mobil bilgi sistemleri, mobil uygulama ve bağlı cihazların çoğalması, veri ve kimlik hırsızlığı fırsatlarını artırmaktadır. Kullanıcılar, kişisel veri ve hesap bilgileri verisinin korunmasından emin olmadığı sürece, bu sistemleri kullanmakta çekingen davranabilmektedir. Kim, Mirusmonov, v.d. (2010) ve Linck, Pousttchi, v.d. (2007) çalışmalarında, mobil ödeme sistemlerinin benimsenmesinde en önemli engel olarak ortaya güvenlik çekincelerinin çıkmakta olduğu sonucuna ulaşmışlardır. Aydın ve Burnaz (2016) ise çalışmalarında güvenlik çekincelerini ortadan kaldırabilecek şekilde iletişim faaliyetlerinin gerçekleştirilmesinin mobil ödeme kullanma niyetini iyileştirme açısından anlamlı sonuçlar getireceğini belirtmişlerdir.

Bu çalışmada öncelikle mobil ödeme ekosistemi ve ekosistemdeki paydaşlar ele alınarak açıklanmaktadır. Sonraki bölümde mobil ödeme çeşitleri, ödeme verisinin sakladığı yere ve mobil ödeme iletişim teknolojisine göre sınıflandırılmakta ve incelenmektedir. Dördüncü bölümde mobil ödeme sistemlerinde güvenlik ele alınarak, öneriler ortaya konmaktadır. Beşinci bölümde ise çalışma genel çerçevesi ortaya konarak sonuçlandırılmaktadır.

2. Ekosistem ve Sistemin İşleyişi

Geleneksel kartlı ödeme sistemlerinde kart çıkaran kuruluşun görevi, hem kartı çıkaran hem de kart çıkarma sürecini kontrol eden olması dolayısıyla daha kolaydır. Ancak, mobil ödeme sistemlerinde işler biraz daha karmaşık hale gelmektedir. Çünkü mobil ödeme sağlayıcısı diyebileceğimiz kuruluşların güvenli unsur üzerinde doğrudan bir etkileri bulunmamakta, sadece aracılık etmektedirler. Bu nedenle kart çıkaran kuruluşlar, kendi mobil ödeme uygulamasının güvenli unsura iletilmesi ve kullanılabilmesi için bir ya da birden fazla üçüncü tarafla anlaşma yapmak zorunda kalabilmektedir.

Mobil ödeme sisteminde rol alan paydaşlar çeşitli Kanunlarda tanımlanmış olmakla birlikte sistemin tam olarak anlaşılabilmesi için Kanunlarda yer almayan çeşitli tanımlara da ihtiyaç duyulmaktadır. Bu bağlamda değerlendirildiğinde, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları hakkında Kanun'un (Kanun) Tanımlar başlıklı 3. Maddesinde:

Gönderen; "Kendi ödeme hesabından veya ödeme hesabı bulunmaksızın ödeme emri veren gerçek veya tüzel kişi" olarak tanımlanmıştır. Mobil ödemeyi gerçekleştiren paydaştır. Müşteri, ödemenin yapıldığı kart, hesap veya mobil cihazın sahibi olup aynı zamanda mobil hizmetler için abonelik ilişkisi bulunmaktadır.

Alıcı; "Ödeme işlemine konu fonun ulaşması istenen gerçek veya tüzel kişi" olarak tanımlanmıştır.

Alıcı, bir işyeri olabileceği gibi gerçek bir kişi de olabilmektedir. Mobil ödemeler kapsamında, alışveriş yapılırken ödeme kabul eden paydaş işyeri, P2P (Person to Person/Kişiden Kişiye) para transferinde ise gerçek kişi olmaktadır. Bu çalışmada, "işyeri" ifadesi ile her iki durum da kapsanmaktadır. Müşterinin ve mobil ödeme aracının fiziksel olarak işyeri ile aynı ortamda bulunduğu ve P2P kapsamına girmeyen ödemelerin gerçekleşebilmesi için, işyerinin ödemeyi kabul edebilecek bir cihaz bulundurması gerekmektedir. Bu cihaz doğrudan Üye İşyeri Anlaşması Yapan Kuruluş ile veya bu kuruluşa hizmet sunan bir üçüncü parti kuruluş ile bağlantı kurarak

ödemeyi kabul eder. Çalışmamızda bu cihaz "POS (Point Of Sale/Ödeme Noktası)" olarak ifade edilmiştir. Bu noktada NFC destekli geleneksel POS cihazlarının yanı sıra sanal mobil POS adı verilen mobil cihazlar üzerinde çalışan ve ödeme kabul eden uygulamalar kullanılabilmektedir. Sanal Mobil POS, mobil bir cihaza bir uygulamanın yüklenmesi ve kart okuyucunun mobil cihaza takılması ile çalışmaktadır. Bu sisteme örnek olarak "Square Register" verilebilir (Wang, Hahn, v.d., 2016).

İşyerinin mobil ödemeler için bir diğer önemli fonksiyonu da mobil ödeme aracına eklenebilen sadakat kartı, hediye kartı, indirim, fırsat veya diğer pazarlama araçlarını sağlamaktır. Müşterinin mobil ödeme aracına işyerinin sağladığı bu gibi pazarlama mekanizmalarını da yükleyebilmesinin, mobil ödeme sistemlerinin kullanımını artıracağı düşünülmektedir.

Ödeme hizmeti kullanıcısı; "Gönderen, alıcı veya her ikisi sıfatıyla belirli bir ödeme hizmetinden faydalanan gerçek veya tüzel kişi" olarak tanımlanmıştır.

Ödeme aracı; Ödeme hizmeti sağlayıcısı ile kullanıcısı arasında belirlenen ve ödeme hizmeti kullanıcısı tarafından ödeme emrini vermek için kullanılan kart, cep telefonu ve benzeri kişiye özel araçtır.

Kişisel güvenlik bilgileri; "Ödeme aracı ile işlem gerçekleştirirken kullanılabilecek şifre, son kullanma tarihi, güvenlik numarası gibi ödeme aracını ve ödeme aracı kullanıcısının kimliğini belirleyici bilgiler" olarak tanımlanmıştır.

Ödeme verisi de denilebilecek kişisel güvenlik bilgileri; ödeme esnasında müşterinin kimliğini doğrulamak için kullanılan hesap bilgisi, kart verisi, ödeme veya kimlik doğrulama aracı başvurusu için kullanılan veriler ve değişikliği durumunda kart hamilinin ödemeyi onaylamasını veya ödeme hesabını kontrolünü etkileyebilecek (müşteri tarafından tanımlanan limitler ve kısıtlar gibi) parametreler gibi hassas bilgilerdir.

Mutabakat Kuruluşu (Clearing and Settlement Mechanism - CSM); "Nezdinde mutabakat hesabı bulunduran ve gerektiğinde katılımcıya mutabakat amacıyla kredi verebilen kuruluş" olarak tanımlanmıştır. Mobil ödeme sonrasında kartlı sistem kuruluşları arasındaki finansal mutabakatı sağlayan paydaştır.

Ödeme Kuruluşu; Ödeme hizmeti sağlamak ve gerçekleştirmek için 6493 sayılı Kanun kapsamında yetkilendirilmiş tüzel kişidir. Kartlı Sistem Kuruluşu, Ağ Operatörü, Mobil Ödeme Hizmet Sağlayıcı, Güvenli Unsur Sağlayıcı, Üye İşyeri Anlaşması Yapan Kuruluş ve varsa Güvenilir Servis Sağlayıcı, Ödeme Geçiş Sağlayıcısı kuruluşla-

rının geneline verilen isimdir.

Bunlara ek olarak, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun Tanımlar başlıklı 3. Maddesinde:

Kartlı Sistem Kuruluşu; Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye işyeri anlaşması yapma yetkisi veren kuruluşlardır.

Kart Çıkaran Kuruluş (Issuer); Banka kartı veya kredi kartı düzenleme yetkisini haiz bankalar ile diğer kuruluşlardır.

Üye İşyeri Anlaşması Yapan Kuruluş (Acquirer); Banka kartı veya kredi kartı kabulünü sağlamak amacıyla işyerleriyle anlaşma yapan bankalar ya da kuruluşlardır. Bazı mobil ödeme mekanizmalarında, üye işyeri anlaşmasını Mobil Ödeme Hizmet Sağlayıcı kuruluş gerçekleştirmektedir.

Üye İşyeri (Merchant): Üye işyeri anlaşması yapan kuruluşlar ile yaptığı sözleşme çerçevesinde ödeme hizmeti kullanıcısına mal ve hizmet satmayı veya nakit temin etmeyi kabul eden gerçek veya tüzel kişidir.

Elektronik Haberleşme İşletmecisi (Ağ Operatörü - Mobile Network Operator/ Internet Service Provider - MNO/ISP); 5809 sayılı Elektronik Haberleşme Kanunu'nda "İlgili alt yapıya ilişkin gerekli elektronik haberleşme tesislerinin kurulması, kurdurulması, kiralanması veya herhangi bir surette temin edilmesiyle bu tesisin diğer işletmecilerin veya talep eden gerçek veya tüzel kişilerin kullanımına sunulması" olarak tanımlanmıştır.

Mobil ödemelerde fiziksel altyapıyı sağlayan paydaştır. Ağ operatörü, fiziksel ve mobil ağ altyapının işletilmesi, mesajların güvenli bir şekilde iletilmesi, mobil ödemede telefon numarası kullanılıyorsa bunun yönetimi ile mobil cüzdan ve mobil ödeme uygulamalarının UICC/SIM (Universal Integrated Circuit Card/ Subscriber Identification Module) yoluyla müşterinin mobil cihazına iletilmesinden sorumludur.

Yukarıda verilen tanımlara ek olarak sistemin daha iyi anlaşılması için aşağıdaki tanımlara da ihtiyaç olduğu düşünülmektedir.

Mobil Cüzdan; Birden fazla mobil ödeme uygulamasının veya farklı özellikteki kartların bir arada tutulduğu mobil ödeme mekanizmasıdır.

Mobil cüzdanlar internete bağlı ise "sıcak cüzdan", değilse "soğuk cüzdan" olarak ikiye ayrılır. Soğuk cüzdanların, sıcak cüzdanlara göre daha güvenli olduğu kabul

edilmektedir. Sıcak cüzdanlar, bilgisayara indirilerek kurulan masaüstü, çevrimiçi olarak bulutta çalışan cüzdanlar ve cep telefonuna indirilerek kullanılan mobil uygulamalar olarak kullanılabilir. Buna karşılık soğuk cüzdanlar ise donanım ya da çevrimiçi olarak üretilen kâğıt üzerinde saklanılarak kullanılır (Güven ve Şahinöz, 2018). Mobil cüzdanlarda birden fazla kredi ve banka kartı depolanabilmektedir. Bu, kullanıcıların cüzdan ve kart taşıması ihtiyacını azaltır. Dünya genelinde mobil cüzdanlara örnek olarak Apple Wallet, Google Pay, PayPal, Samsung Pay, AliPay (Ashay, Joon, 2016); Türkiye'de ise BKM Express, Mobilexpress ve Shopamani SmartWallet verilebilir.

Mobil Ödeme Hizmet Sağlayıcısı (Mobile Payment Service Issuer); "Ödeme Hizmet Sağlayıcı (Mobile Payment Service Issuer); Mobil ödeme uygulamasının sağlanmasından sorumludur. Uygulama ve kart bilgileri kullanılan mobil ödeme metoduna göre mobil cihaz bünyesindeki güvenli unsurda (SE – Secure Element), fiziksel sunucularda (Secure Server) ya da bulut ortamında saklanabilmektedir.

Güvenli Unsur Sağlayıcı (Secure Element Issuer); Mobil ödeme uygulaması ve kart verisi mobil telefon bünyesindeki güvenli unsurda saklandığı hallerde, bu güvenli unsuru sağlayan, bakımını ve güncelleştirilmesini gerçekleştiren paydaştır.

Güvenilir Servis Sağlayıcı (Trusted Service Manager - TSM); Mobil Ödeme Hizmet Sağlayıcı, Kart Çıkaran Kuruluş veya Üye İşyeri Anlaşması Yapan Kuruluş adına hareket eden ve her üçüne de hizmet sunarak farklı ödeme kuruluşlarının birlikte çalışabilirliğini sağlayan paydaştır. Pratikte, uygulama yaşam döngüsü yönetimi, şifreleme anahtarlarının yönetimi gibi görevleri de yerine getirebilmektedir. Genelde bir üçüncü parti kuruluşu olmakla birlikte, Güvenilir Servis Sağlayıcı fonksiyonlarının diğer paydaşlarca gerçekleştirilebildiği uygulamalar da mevcuttur.

Ödeme Geçiş Sağlayıcısı (Payment Gateway); İşyeri adına mobil ödemelerin yetkilendirilmesini sağlayan üçüncü taraf kuruluştur.

Bulut; Kullanıcı kişisel bilgileri, hesap bilgileri veya ödeme bilgileri gibi verilerin ödeme kuruluşunun kendi ağındaki sunucularda veya hizmet alınan üçüncü taraf sunucularda saklandığı ortamdır.

Bu çalışmada güvenliği sağlanmış bulut ifadesi ile BDDK tarafından yayınlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Yönetmelik Taslağı 29. Madde 11. Fıkrada yer alan " Banka, bir dış hizmet olarak bulut bilişim hizmetlerini de kullanabilir. Bu şekilde alınacak bulut hizmeti, tek bir bankaya tahsis edilmiş donanım ve yazılım kaynakları üzerinden özel bulut hizmet modeliyle alınabileceği gibi birden fazla banka arasında donanım ve yazılım kaynaklarının fiziken paylaşıldığı an-

cak mantıksal olarak her bankaya ayrı kaynaklar atayan ve sadece bankalara hizmet veren topluluk bulutu hizmet modeliyle de alınabilir

Ana bankacılık uygulaması, kredi ve kredi kartı uygulamaları ile ödeme hizmeti gibi faaliyet konularında topluluk bulutu hizmet modeliyle dış hizmet alınabilmesi Kurulun iznine tabidir." Hükmünde yer aldığı gibi özel (private) bir bulut hizmeti ya da sadece banka veya finansal kuruluşlara hizmet veren topluluk (public) bulut ifade edilmektedir. Söz konusu hükmün düzenlenmesinin son derece isabetli olduğu düşünülmektedir.

Token/Tokenization (Simge/Simgeleştirme); Kart bilgisi, kullanıcı bilgisi, ödeme bilgisi gibi hassas ödeme verilerinin matematiksel bir fonksiyon vasıtasıyla üçüncü kişiler tarafından anlaşılmayacak şekilde rastgele üretilmiş, tekil ve tek yönlü (ters algoritmalarla orijinal verinin elde edilemediği) bir değere dönüştürülmesidir. Veri iletimi esnasında hassas veriler yerine token değeri iletilir.

Kişiden Kişiye Ödeme (Person-to-person payments (P2P)); Kullanıcıların banka hesapları veya kredi kartı hesaplarından başka bir kişinin hesabına internet veya mobil telefonları aracılığıyla para aktarabildiği çevrimiçi teknolojidir (InvestingAnswers, 2019).

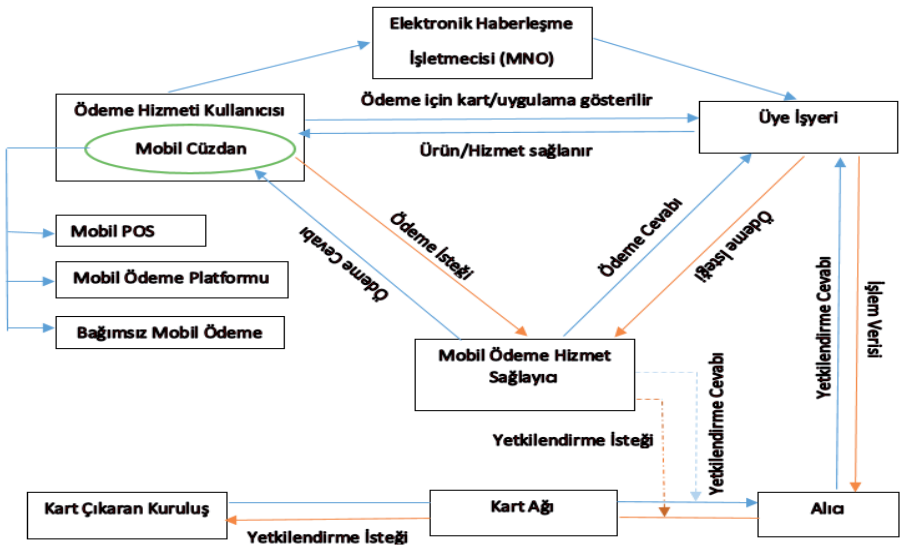
Tanımları yapılan paydaşlar birbirinden ayrı olabildiği gibi bazı paydaşlar tek kuruluş bünyesinde toplanabilmektedir. Ayrıca sıralanan paydaşlar haricinde kullanılan mobil ödeme teknolojisine göre Güvenli Unsur Üreticisi (SE Manufacturer), Mobil Ödeme Uygulaması Geliştiricileri ve Güvenilir Mobil Ödeme Hizmet Sağlayıcıları da ekosistem içerisinde yer alabilmektedir.

Bir mobil ödeme işlemi farklı uygulama ve metotlarda birçok farklılık gösterebilecek olmakla birlikte özetle şu şekilde gerçekleşmektedir. Mobil ödeme hizmetinden faydalanmak isteyen kişi mobil ödeme hizmet sağlayıcısına kayıt olarak müşteri (kullanıcı) haline gelir. Müşteriye ilgili mobil ödeme uygulamasının güvenli bir şekilde iletilmesinden mobil ödeme hizmet sağlayıcı, ağ operatörü ve varsa güvenli unsur sağlayıcı ile güvenilir servis sağlayıcı sorumludur. Herhangi bir mal veya hizmet sağlayan ticari firma, üye işyeri anlaşması yapan kuruluşla sözleşme imzalayarak ve kabul etmeyi planladığı mobil ödeme teknolojilerinin gerektirdiği donanım yatırımını yaparak işyeri haline gelir.

Müşteri fiziksel olarak veya internet üzerinden bir işyerinden alışveriş yaptığında (Şekil 1), mobil ödeme uygulamasında bulunan müşterinin kart bilgisi güvenli unsur kullanılması halinde kart çıkaran kuruluş, bulut teknolojisi kullanılması halinde ise

mobil ödeme hizmet sağlayıcısı ve sonrasında kart çıkaran kuruluş tarafından doğrulanır. Bütün bu aşamalarda her paydaş ilettiği verinin şifreli olarak iletilmesinden sorumludur. Ancak, veri iletiminin gizlilik, bütünlük ve erişilebilirliğinden ağ operatörü sorumludur. İşlem sonunda ödeme meblağı kart çıkaran kuruluş tarafından müşteriden tahsil edilir ve üye işyeri anlaşması yapan kuruluş tarafından işyerine ödenir. Bu iki paydaş arasındaki mutabakat ve finansal netleştirmeler mutabakat kuruluşu tarafından yapılır.

Şekil 1. Mobil Ödeme Ekosistemi Çalışma Şeması



Kaynak: Wang, Hahn, v.d., (2016)

3. Mobil Ödeme Çeşitleri

Akıllı telefonların sunduğu kabiliyetler sayesinde mobil ödemelerde çeşitlilik oldukça fazladır. Her bir mobil ödeme uygulaması farklı ek özelliklerle müşteri çekmeye ve işyerleri ile anlaşma yapmaya çalışmaktadır. Halen gelişmekte olan bir alan olması sebebiyle, mobil ödemelerde genel kabul görmüş bir sınıflandırma ve terminoloji henüz oluşmamıştır. Mobil ödemeleri; ödeme şekline, riski taşıyan paydaşa, ödeme verisinin saklandığı yere ve mobil cihaz ile POS arasındaki iletişim teknolojisine göre sınıflandırmak mümkündür.

Ödeme şekline göre mobil ödemeler üçe ayrılabilir. Bunlardan ilki, P2P (person to person) mobil ödemelerdir. Bu tip ödemelerde gönderen, alıcının telefon numa-

rası, e-posta adresi gibi gizli olmayan ve tekil olarak alıcıyı tanımlayacak bir bilgiyi kullanarak gerçek bir kişi olan alıcıya para iletilir. İkinci ödeme şekli, uzaktan mobil ödemelerdir. Bu yöntemde, müşteri POS terminali ile sanal etkileşim kurarak ödemeyi gerçekleştirir. Üçüncü ödeme şekli ise temassız mobil ödemelerdir. Müşteri mobil telefonunu kullanarak POS cihazından ödeme yapar.

Bir diğer sınıflandırma da riski taşıyan paydaşa göre yapılmaktadır. Mobil ödemeleri buna göre üç başlık altında incelemek mümkündür: GSM operatörünün riski üstlendiği yapılar, bir kartlı sistem kuruluşunun riski üstlendiği yapılar ve müşterinin riski üstlendiği yapılar (Carr, 2010).

GSM operatörünün riski üstlendiği yapılarda, müşterinin mobil telefonu ile yaptığı alışverişlere ilişkin satın alma bedeli operatör tarafından müşterisinin aylık faturasına yansıtılmaktadır. Bu ödeme yöntemi genellikle sanal ortamdaki dijital ürünlerin alımında kullanılmaktadır. Mobil cihazlarda kullanılan uygulamalar için kredi kartı bilgisini paylaşmak istemeyen veya güvenlik sebebiyle ödeme onayının birkaç adımda gerçekleştirilmesinden şikâyet eden kullanıcılar için tercih edilebilir bir ödeme alternatifi olduğu söylenebilir. Ancak satışı gerçekleştiren işyerinden kesilen komisyon oranının diğer ödeme hizmeti sağlayıcılarına göre çok daha yüksek olması ve bu maliyete satıcıların katlanması sebebiyle satıcılar tarafından dezavantajlı olarak görülmektedir. Ayrıca, mobil operatörlerin abonelerine kredi sağlama gibi bir fonksiyonları bulunmamaktadır. Bu sebeple mobil operatörler hiç bilmedikleri bir işe girmekte isteksiz davranabilmektedir. Yüksek ücretli SMS (yarışma, bağış amaçlı v.b.) ve yüksek ücretli aramalar da bu kapsamda ele alınmaktadır.

Bir kartlı sistem kuruluşunun riski üstlendiği yapılarda, müşterinin mobil telefonu ile yaptığı alışverişlere ilişkin satın alma bedeli kadar kredi kartı borçlandırılıp işyerinin hesabına transfer edilerek ödeme gerçekleştirilir. Alışveriş bedeli, müşterinin kredi kartı ekstresine yansıtılır. Dünya genelinde en fazla tercih edilen mobil ödeme yöntemidir. Müşterinin ödeme güçlüğü yaşaması durumuna ilişkin riski, kredi kartını çıkaran kuruluş üstlenmiştir. Müşterinin riski üstlendiği yapılarda, müşterinin ön ödemeli kartı, banka kartı veya banka hesabı kullanılmaktadır. Alışverişe ilişkin ödeme, alışveriş esnasında tahsil edilmektedir.

Güvenlik perspektifinden bakıldığında ödeme verisinin güvenli bir şekilde saklanması ve iletilmesi önem arz etmektedir. Bu çalışmanın odağında güvenliğin yer alması sebebiyle ödeme verisinin saklandığı yere göre ve ödeme esnasında kullanılan iletişim teknolojisine göre sınıflandırmalar ayrı başlıklar altında ele alınmıştır.

3.1. Ödeme Verisinin Saklandığı Yere Göre

Ödeme verisinin saklandığı yer, veri mahremiyetinin ve ele geçirilmesi durumunda müşteri bilgisi haricinde ödeme yapılabilecek verilerin gizliliğinin sağlanması adına önem arz etmektedir. Ödeme verisinin saklanacağı yer aynı zamanda, fiziksel güvenliğin sağlanmasındaki sorumluluğun sahibinin de belirlenmesi anlamına gelecektir. Mevcut ödeme sistemleri göz önüne alındığında ödeme verileri, mobil cihaz içerisinde yer alan güvenli unsurda veya bulut ortamında saklanabilmektedir.

3.1.1. Mobil Ödeme Cihazı (Güvenli Unsur)

Ödeme verisi mobil telefon bünyesinde yer alan güvenli unsurda (secure element) saklandığında, verinin saklanma esnasındaki fiziksel güvenliği, servisi kullananın sorumluluğundadır. Güvenli unsur, mobil cihazlar içerisinde güvenilir operasyonların gerçekleştirilebildiği ve ödeme bilgileriyle kriptografik anahtarların muhafaza edilebildiği izole bir alan sunan, kurcalanmaya karşı önlemler barındıran, çip seviyesinde bir güvenlik bileşenidir. Uygulama yöntemi olarak günümüzde 3 farklı formda güvenli unsur kullanımı öne çıkmaktadır (GlobalPlatform, 2018).

- Gömülü güvenli unsur: Cep telefonu üreticisi firma tarafından üretim sürecinde cihaza yerleştirilen ve kontrolü yine üreticide olan bir devre parçasıdır. Son dönemlerde birçok akıllı telefon üreticisi NFC destekli modelleri piyasa sürerken, bunlarla ödemeyi kabul eden POS cihazları da işyerlerinde yer bulmaya başlamıştır. Güvenli unsurun gömülü olması cihazla uyum garantisi getirirken, en büyük dezavantajı bir cihazdan diğerine taşınabilir olmaması olarak gözükmektedir.

- Geliştirilmiş SIM (Subscriber Identity Module) kartı: Standart SIM kartın yerini alan ve içinde güvenli unsur devresini barındıran geliştirilmiş SIM kartları -diğer bir adıyla Universal Integrated Circuit Card (UICC)- mobil ağ operatörleri tarafından sağlanıp son kullanıcıya sunulmaktadır. Mobil ağ ve cihaz uyumu garantisi olan bu kullanım formunda, kartlı sistem kuruluşu ile GSM operatörü arasında bir anlaşma yapılması gerekmektedir.

- MicroSD kart: Birincil kullanımı mobil cihazlarda bellek kapasitesini arttırmak olan MicroSD kartların güvenli unsur devresi barındıran versiyonları mobil ödemeyi desteklemektedir. Bu ürünler genellikle hizmeti düzenleyen banka tarafından sağlanmakta ve kontrol edilmekte olup bu servisi destekleyen telefonlara takılmak üzere kullanıcılara dağıtılmaktadır. Bankaların geleneksel kart düzenleme ve dağıtım yöntemini sürdürebilmesi ve yerleşik olarak NFC

desteği bulunmayan MicroSD yuvalı telefonlarda kullanılabilmesi avantaj olarak gözükmektedir. Buna karşın MicroSD yuvası bulunmayan telefonlarda kullanılamaması ve yuva bulunan cihazlarda da fazladan bir yer işgal etmesi yaygınlaşması yolunda engel teşkil etmektedir.

Mobil ödeme uygulamasının mobil cihaz içerisinde yer alan güvenli unsurda tutulmasına dünyadan örnek olarak Kenya, Hindistan ve Afganistan'da kullanılan MPESA ile ABD'de kurulu ISIS ve Google Wallet 1.0 verilebilir. MPESA ve ISIS güvenli unsur olarak "gelişmiş SIM kart" kullanırken, Google Wallet 1.0 "gömülü güvenli unsur" kullanmaktadır.

3.1.2. Bulut

Bu ödeme sisteminde ödeme verisi bulut ortamında tutulmakta ve mobil cihaza sadece ödeme esnasında buluta bağlanmak için aracılık fonksiyonu yüklenmektedir. Uygulamadan uygulamaya farklılık göstermekle birlikte saklanılan ödeme verileri veya bu veriler kullanılarak elde edilen yapılar (token), işlem esnasında müşterinin mobil telefonuna veya işyerine iletilebileceği gibi hiçbirisine iletilmeden ödeme işlemi arka planda da gerçekleştirilebilmektedir.

Ödeme verilerinin mobil telefonda tutulduğu durumdan farklı olarak, bulutta ödeme verilerinin tutulmasına ilişkin genel kabul görmüş standartlar henüz oluşturulmamıştır. Bunun sebeplerinin başında güvenli olarak bulut üzerinde ödeme verilerinin saklanmasına ilişkin teknolojilerin sürekli gelişmekte ve değişmekte olması gelmektedir. Ayrıca bulut üzerinde veri saklama imkânları mobil telefonda olduğundan daha fazladır ve her uygulama, pazarda kendisini farklı bir yere oturtabilmek için farklı özellikler barındırmaktadır.

Mevcut uygulamalardan, PayPal, Square, Seamless, LevelUp, Venmo, GoPago, QwickCodes, Cloud Zync, Dwolla ve MCX gibi şirketler mobil ödeme bilgisini saklamak amacıyla bulut tabanlı yaklaşımı benimsemişlerdir. Bu konuda en ilginç örneklerden bazıları da Facebook, Twitter, Instagram ve WeChat gibi sosyal medya kapsamında sunulan mobil ödemelerdir.

Ödeme verisinin bulutta saklandığı durumlarda, mobil ödeme sistemi sağlayıcıları mobil telefon üreticilerine ve GSM operatörlerine daha az bağımlı olmaktadır. Öte yandan ödeme verisinin mobil telefon bünyesindeki güvenli unsurda saklanması durumunda ise, telefonun internet bağlantısı, şarj ve çekim durumlarına bağlı olmaksızın müşteri tarafından ödeme gerçekleştirilebilmektedir.

3.2. İletişim Teknolojisine Göre

Gelişen teknolojilerden faydalanarak her geçen gün mobil cihaz ile ödemeye olanak sağlayan yeni kimlik doğrulama yöntemleri geliştirilmektedir. Hatta uygulamalar esnek olabilmek adına müşteriye birden fazla yöntemden faydalanma imkânı sunabilmektedir. Günümüzde var olan uygulamalar dikkate alındığında, ödeme esnasında müşterinin kimlik doğrulama verilerinin iletişiminde kullanılan teknolojiye göre mobil ödemeler, NFC, QR Kodu, SMS/USSD ve Internet olarak dört başlık altında incelenmiştir:

3.2.1. NFC

NFC (Near Field Communication), Türkçe adıyla "Yakın Alan İletişimi", verilerin bir cihazdan diğerine 10 cm'den daha kısa bir mesafede kablosuz olarak aktarılmasını sağlayan bir teknolojidir. NFC, sadece NFC çipler birbirine çok yakın olduğunda çalışan özel bir RFID radyo frekansı (13.56 MHz) kullanır. NFC özelliğine sahip cihazlar, birbirine yaklaştırılarak aktif hale geldiğinde, NFC çipleri bir ödemeyi tamamlamak için şifrelenmiş verileri değiştirir. Bu aktarımın gerçekleştirilebilmesi için söz konusu cihazlarda NFC yongalarının ve antenlerin bulunması gerekir. İki cihaz arasındaki kablosuz veya "temassız" bağlantı, kablosuz izleme uygulamalarında kullanılan radyo frekansı tanımlama (RFID) etiketlerine benzer radyo dalgalarını kullanır.

NFC teknolojisi, mobil telefonun fiziksel olarak bir POS cihazı ile aynı ortamda bulunduğu ödemelerde kullanılmaktadır. Müşterinin ödemeyi tamamlaması için NFC desteği bulunan mobil telefonunu okuyucu modüle yaklaştırması yeterlidir. Bu şekilde gerçekleştirilen çoğu işlemde PIN girilmesi beklenmemektedir, zira NFC'nin pazarlama stratejisinde işlemin çabukluğu ve pratiklik önemli bir yer tutmaktadır. Buna karşın, belirli limitin üzerinde alımlarda veya günlük olarak belirlenen limitlerin aşılması hallerinde güvenliği artırmak amacıyla ödemenin onaylanabilmesi için PIN doğrulamasının da yapılması güvenliği artıracaktır.

NFC çipi; kart (pasif mod), okuyucu (aktif mod) ya da her iki fonksiyonu yerine getirebilen mobil bir cihaz olarak düşünülebilir. Aktif mod NFC cihazının kendi RF (Radio Frequency) sinyalini oluşturması, pasif mod ise başka bir cihaz tarafından oluşturulmuş RF sinyali ile çalışması şeklinde tanımlanabilir. NFC kullanan mobil cihazlar aktif ve pasif mod arasında kolaylıkla geçiş yapabilmektedir. İki NFC cihazının karşılıklı olarak aktif modda çalıştığı aktif-aktif iletişimin yanı sıra bir cihazın aktif modda diğer cihazın pasif modda çalıştığı aktif-pasif iletişim mümkün olmaktadır. Aktif-aktif çalışma modunda her iki cihaz da kendi enerjisini kullanarak RF sinyalini

üretebilmekte, aktif-pasif çalışma modunda ise aktif cihazın ürettiği enerji her iki cihaz tarafından kullanılmaktadır. İletişim esnasında iletim kanalı her iki cihaz arasında değişmeli olarak kullanılmaktadır. Her cihaz mesaj göndermek için diğer cihazın oluşturduğu RF alanını kapatmakta ve kendisi sinyal üreterek göndermektedir. Aktif - aktif çalışmada, her iki cihaz da kendi enerjisini ve RF sinyalini kendisi ürettiği ve daha yüksek modülasyon güçleri harcandığı için daha yüksek veri iletişim hızlarına ulaşılabilmektedir.

NFC ödeme süreci, kullanıcıların kolay, hızlı ve güvenli ödeme yapmasını sağlamaktadır. Bu nedenle, Apple Pay ve Google Pay gibi NFC tabanlı ödemeler, hızlı bir şekilde tercih edilen bir tüketici ödeme yöntemi haline gelmektedir. Mobil ödemeli POS (mPOS) pazarı, geleneksel POS pazarından daha hızlı büyümektedir ve Berg Insight projeksiyonlarına göre dünya genelinde 2017 yılında 34 milyon adet olan mPOS terminali sayısı, 2022 yılında 86 milyon adede ulaşacaktır (Berg Insight, 2017).

Bununla birlikte gelişen teknolojiler sayesinde NFC kabiliyeti içeren cep telefonlarının POS cihazı olarak kullanımı da görülmektedir. Ancak bu şekilde kullanımlar ödeme ekosisteminin başlangıç noktasında yer alan cihazların güvenlik riskini artırmaktadır. Mobil cihazların güvenliğini sağlamak geleneksel POS'lara göre daha zor olabilmektedir. Bu durum fiziksel atak vektörlerine ek olarak dijital saldırılara da olanak veren bir yüzey haline gelmektedir.

3.2.2. QR Kodu

QR (Quick Response) kodlar, 1994 yılında keşfedilmesine karşın son yıllarda kullanımı yaygınlaşan ve akıllı telefonlara bilgi enjekte etmek amacıyla da kullanılabilen 2-boyutlu (matris) barkotlardır. 2D barkodlar; yaygın tek boyutlu barkodların gelişmiş, daha fazla kapasiteye sahip ve küçültülmüş formlarıdır. 2D barkodlar; daha fazla bilgi taşımakta, veri kaybını önleyen çok güçlü güvenilirlik garantisi sunmakta, hem yatay hem de dikey yönde bilgi içermeleri nedeniyle her iki yönde okunabilmektedirler (Ghiron, Medaglia, v.d. 2009). 2D barkodların kullanımı yoğun olarak mobil cihazlarla olduğundan "mobil barkod" ismi yaygın olarak kullanılmakta (Aygören ve Varnali, 2011), uygun bir yüzeye uygulanması, "mobil kodlama" ya da "mobil etiketleme" olarak adlandırılmaktadır. Mobil kodlama; mobil cihazlar yoluyla ve iki boyutlu barkod kullanılarak yerleşik kameralı bir mobil cihaz tarafından okunabilir veri elde etme sürecidir (Varnali, Toker v.d. 2011). En yaygın kullanılan 2D barkodlar ise açık-kaynak platformlar olan QR kodlardır (Bozkurt ve Ergen, 2011).

Bir ürüne, metne veya URL (Uniform Resource Locator)'ye ilişkin QR kod, ilgili olan bütün bilgiyi gömülü olarak barkodunda taşımaktadır. Örneğin, bir web sitesinin URL'sine karşılık gelen QR kod, uygun yazılımın yüklü olduğu bir akıllı cihazın kamerasıyla tarandığında, siteye erişim sağlanabilmektedir. Geleneksel barkotlar sadece sayıları temsil ettiğinden, anlamlı bir bilgiye erişmek için bir tablodan barkoda karşılık gelen tanıma bakılması gerekmektedir. Buna karşın QR kodlarda anlamlı veri, direkt olarak barkodun içeriğinde saklanmaktadır.

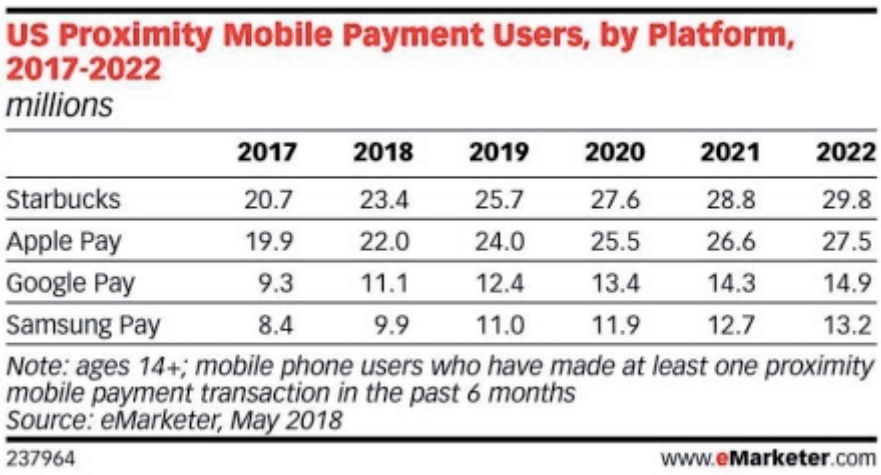
Mobil ödemelerde iletişim teknolojisi olarak QR kodunun kullanılması üç şekilde gerçekleşebilir. Bunlardan ilki, işyeri tarafından üretilen QR kodunun müşterinin mobil telefonu tarafından okunması ve ödemeye ilişkin bilgilerin (işyeri, tutar, vb.) müşterinin mobil telefonuna iletilmesi şeklinde gerçekleşir. İkincisi, bir QR kodun müşteri tarafından mobil telefona okutulması ile telefonun bir internet sayfasına yönlendirilmesi sonrasında müşterinin alışveriş yapıp ödeme gerçekleştirmesi şeklindedir. Üçüncüsü ise, müşterinin ödeme bilgisini (kredi kartı, sadakat kartı gibi) içeren QR kodunun işyeri tarafındaki QR kod tarayıcısı tarafından okunması şeklindedir.

QR kod kullanımının cazip olmasının ana sebebi, herhangi bir akıllı telefonla ve işletim sistemiyle kullanılabilmesi ve satış noktası tarafında gereken tek yatırımın 2 boyutlu bir barkot okuyucu ve basit bir yazılım güncellemesi olmasıdır. Kullanım kolaylığı ve akıllı telefonlar vasıtasıyla birçok birey için ulaşılabilir olmasının da getirisiyle, QR kodlar çok sayıda başarılı mobil ödeme sisteminin tecrübe edilmesini sağlamışlardır.

Bunun yanı sıra QR kod kullanılarak yapılan mobil ödemelerin en başarılı örnekleri arasında Çin'de çok yaygın kullanılan Alipay ve WeChat yer almaktadır. Her iki uygulamada hem üye işyeri hem de kullanıcı tarafında QR kod yer alan ödemeleri kabul etmektedir. Alipay, Ali ve Taobao e-ticaret platformları sayesinde çok büyük bir pazar payına sahiptir. Wechat ise kullanıcı taleplerini iyi takip eden bir sosyal platformdur. Her iki uygulama da yaptıkları promosyonlar ve güven sağlayıcı yenilikçi teknolojileri ile müşterileri başarılı bir şekilde etkilemiştir. Bu sayede Çinli kullanıcılar ödemelerde QR kodu ile alışverişe olumlu şekilde yaklaşmaktadır (Zhang, 2018).

Bunun yanı sıra QR kod kullanılarak yapılan mobil ödemelerin en başarılı örnekleri arasında Starbucks uygulaması da yer almaktadır. Starbucks'lar fiziksel satış noktası işlemlerinde en çok sayıda mobil ödemenin gerçekleştirildiği yerler olup, penetrasyon 2017 sonu itibariyle toplam satışın %30'una ulaşmıştır. EMarketer'in 2018 yılı anketine göre Starbucks mobil ödeme uygulaması, Apple Pay, Google Pay ve Samsung Pay mobil ödeme uygulamalarından daha fazla kullanılmaktadır ve gelecek 4 yılın projeksiyonlarında daha fazla kullanılacağı beklenmektedir (Şekil 2).

Şekil 2. ABD Mobil Ödeme Kullanıcıları



US Proximity Mobile Payment Users, by Platform, 2017-2022

millions

	2017	2018	2019	2020	2021	2022
Starbucks	20.7	23.4	25.7	27.6	28.8	29.8
Apple Pay	19.9	22.0	24.0	25.5	26.6	27.5
Google Pay	9.3	11.1	12.4	13.4	14.3	14.9
Samsung Pay	8.4	9.9	11.0	11.9	12.7	13.2

Note: ages 14+; mobile phone users who have made at least one proximity mobile payment transaction in the past 6 months
Source: eMarketer, May 2018

237964 www.eMarketer.com

Kaynak: Tearsheet, 2018.

Bir diğer başarılı örnek ise LevelUp'dır. ABD'de 200 den fazla marka ile anlaşmalı olan uygulamada, LevelUp'ı telefonuna indiren kişi, daha sonra herhangi bir banka veya kredi kartını buradaki hesabıyla eşleştirir. Bu eşleştirmenin ardından söz konusu kişi için eşsiz bir QR kodu üretilir. Artık bu QR kodu alışverişlerde ödeme yapmak için kullanılabilir. Kişi LevelUp ile ödeme kabul eden bir kafeye gittiğinde telefonundaki uygulamayı açar ve üye işyerindeki QR kod tarayıcısına okutur. Bunun üzerine kasiyer ürün veya hizmetin bedelini tuşlar ve müşteri onayladıktan sonra alışveriş tamamlanır. İşleme ait fiş müşterinin e-posta adresine iletilir.

QR kodlarının sunduğu bir diğer avantaj ise mobil teklifler ve promosyonlar olarak gözükmektedir. Son dönemde akıllı telefonların da yaygınlaşmasıyla popülerleşen mobil kuponlar, hızlı bir şekilde kâğıt kuponların yerini almaktadır. Ayrıca, konuya işletmeler tarafından bakıldığında mobil kuponlar önemli bir maliyet düşüşü sağlarken, tüketiciler tarafında ise kullanım kolaylığı getirmiştir. Örnek olarak, Türkiye'de Boyner Grup tarafından 2015 yılında hayata geçirilen Hopi uygulaması ile QR kod üzerinden ödeme yapılabilmekte, puan biriktirilmekte, indirim ve kampanya kuponları kullanılabilmektedir (Hopi, 2018).

3.2.3. SMS/USSD

Kısa Mesaj Servisi, yani SMS (Short Message Service), GSM teknolojisinin bir parçası olarak geliştirilmiş, mobil telefonlar arası metin mesajlaşmasını sağlayan bir servistir. USSD (Unstructured Supplementary Service Data) ise, GSM standardının bir parçası olarak telefonların servis sağlayıcısına ait sunucularla iletişimini gerçekleştiren

protokoldür. SMS servisinde mesaj gönderen ile alan arasında servis sağlayıcısına ait bir merkez bulunur ve buna bağlı olarak "sakla ve ilet" tekniği kullanılır, mesaj öncelikle merkezde saklanır, alıcı abone GSM ağına bağlandığında kendisine iletilir. Buna karşın USSD protokolü oturum bazlıdır ve bağlantı gerçek-zamanlı olarak gerçekleştirilir. Bu oturumlar süresince gönderilebilecek USSD mesajları en çok 182 karaktere sahip olabilirler. İletişim ağlarına USSD ile bağlantı genelde kullanıcıların haberi olmadan yapılır. USSD kodlar mobil cihazın numara çevirme ekranına belirli bir formatta yazılınca önceden tanımlı işlevi yerine getirmektedir. Telefon görüşmesi başlatmak en klasik USSD işlemlerindendir. İnteraktif uygulamalar göz önüne alındığında, USSD için yanıt süresi SMS'e göre daha kısadır.

Kısa mesaj servisi, bankacılık işlemlerinde de sıklıkla kullanılmaktadır. Kişiler, bilgi alma amaçlı olarak SMS'le bankadaki hesaplarının durumunu sorgulayabilir (ör: bakiye, borç) veya işlem gerçekleştirme istemiyle yine SMS'le ödeme talimatı verebilirler. Öte yandan kullanıcıların aşinalığı yönünden bakıldığında SMS, internet üzerinden gerçekleştirilen bankacılık işlemlerinde, iki faktörlü kimlik doğrulamanın ikinci faktörü (sahip olunan şey - something you have) olarak ülkemizde benimsenmiştir.

Günümüzde, SMS ve USSD teknolojileri bir mobil ödeme yöntemi olarak da kullanılabilmektedir. Bu senaryoda, müşteri mobil cihazını kullanarak abonesi olduğu operatöre kısa mesajla veya USSD koduyla bir ödeme talebi göndermektedir. Karşılığında işleme dair bedel abonenin telefon faturasına yansıtılır veya kullanıyorsa mobil cüzdanından tahsil edilir. Bu süreçte işlemin diğer tarafı, yani üye işyeri de, ödemenin durumu hakkında bilgilendirilir. Bu servis kapsamında müşteriye ait bir teslimat adresi paylaşılmadığı da göz önünde bulundurulduğunda, alınan ürün genellikle dijital olmaktadır. Bilet, müzik ve video gibi SMS/USSD servisi kullanılarak alınabilen ürünler, hizmet sağlayıcısı tarafından çoğunlukla MMS (Multimedia Messaging Service) ile istemciye gönderilir. Ayrıca, ödemenin yapıldığını göstermek amacıyla üye işyerinin fiziksel kontrol gerçekleştirebilmesi için MMS ile bir QR kod/barkod da gönderilebilir.

SMS/USSD ile gerçekleştirilen ödemeler son dönemde popüleritesini kaybederken, yerini diğer mobil ödeme yöntemleri almaktadır. Bu durumun sebeplerinin başında güvenilirlik gelmektedir. Mesajın herhangi bir sebeple gönderilememesi halinde ödeme işlemi gerçekleşmeyeceğinden güvenilir bir yöntem olarak kabul edilmemektedir. İkinci bir etken de güvenliktir. Bu kısım çalışmanın dördüncü bölümünde tartışılacaktır. Bir diğer etken de mesajın yazılıp iletilmesi ve ardından üye işyerinin ödemenin tamamlandığına dair onay alma sürecinin uzun olabilmesidir. Son olarak en önemli etken maliyetin yüksek oluşudur. Servisi kullanan müşteriler kısa mesajlar

için, hizmet sağlayıcısı da multimedya mesaj servisi için ücretlendirilir. Ayrıca GSM operatörleri, ödeme hizmetinden yüksek komisyonlar almaktadır.

3.2.4. Internet

İnternet üzerinden yapılan mobil ödemelerde, ödeme verileri bulutta saklanılmaktadır. Ödeme işlemi esnasında, ödeme verileri veya bu veriler kullanılarak elde edilen token (jeton) vs. gibi unsurlar, müşterinin mobil telefonuna, işyerine veya alışverişe ilişkin bilgilerin mobil cüzdan sağlayıcısına iletilir. Bu işlemlerin sonrasında, ödeme arka planda gerçekleşmektedir. Bu şekilde hassas ödeme verileri ve kişisel bilgilerin herkese açık iletişim ortamlarında iletilmemesi sağlanarak güvenlik artırılmış olacaktır. Hassas ödeme verisinin iletim ortamlarında güvenliğinin sağlanmasının bir diğer yolu da verileri şifreli (encrypted) iletmektir. Ancak bu durumda, iletişimde yavaşlama olabileceği göz ardı edilmemelidir.

Mevcut uygulamalardan PayPal, Square, Seamless, Venmo, GoPago ve Dwolla gibi şirketler bu yaklaşımı benimsemiştir. Mobil ödemelerde en yenilikçi firmalardan olan Square firması, Square wallet uygulamasında getirdiği "Pay with your name – İsminle öde" özelliği sayesinde müşterilerin POS cihazına gitmesine gerek kalmadan ödeme yapmasına imkân tanımıştır. Bu sistemde Square wallet uygulaması müşterinin konum bilgisinden faydalanarak yakınlardaki işyerlerinden oluşan listeyi müşteriye sunar. Alışveriş yapacağı işyerini seçen müşteri işyerine sadece ismini söyler. İşyeri uygulamasındaki müşteri resmini kullanarak müşterinin kimliğini doğrulayan işyeri, tutarı girer ve işlem arka planda bir CNP (Card Not Present – kartın fiziksel olarak değil kart üzerinde basılı olarak yer alan verilerin kullanıldığı ödemeler) işlem gibi gerçekleşir. JPMorgan Chase & Co tarafından üretilen GoPago uygulaması ve eBay'in bir şirketi olan PayPal da benzer ödeme seçenekleri sunmaktadır. Ayrıca PayPal, müşterilerin işyerine ulaşmadan siparişlerini önceden vermesine de olanak sunmaktadır.

Bazı mobil cüzdan uygulamaları, birden fazla iletişim teknolojisini kullanarak, farklı teknolojilerin avantaj ve dezavantajlarını bir araya getirmektedir. Bunun bir örneği olarak, Google, Ağustos 2012'de kullanıma sunduğu Wallet 1.5 uygulamasında hibrit bir mekanizma kullanma yoluna gitmiştir. İşyeri ödenecek tutarı POS cihazına girdikten sonra müşteri, telefonunu NFC'li POS cihazına okutur ve telefondaki sanal kart verisi ile müşterinin kimliği doğrulanmış olur. Daha sonra arka planda standart bir CNP ödemesi ile Google işyerine ödemeyi gerçekleştirir. Son olarak da müşterinin gerçek kartından standart bir CNP ödemesi ile işyerine ödenmiş tutar, Google tarafından tahsil edilir.

Müşterilerin işyerlerine ödeme yaptığı mobil cüzdan uygulamalarında olduğu gibi, P2P ödemelerde de iletişim teknolojisi olarak internet kullanılabilmektedir. Bu ödemelerde en büyük sorun gönderici ile alıcının farklı uygulamalar kullanması halinde alıcıyı tanımlayacak tekil bir yapı oluşturulmasıdır. Seamless, Dwolla ve Venmo firmaları, telefon numarası, e-posta adresi gibi tekil bir ayırt edici ile parayı alacak kişilerin belirlenmesine imkân sunmaktadır. Benzer şekilde, Google'ın Wallet mobil cüzdan servisini Gmail e-posta servisine entegre eden özellik sayesinde e-posta göndererek para transferi yapabilmek mümkündür.

Sosyal medyanın da bir ödeme aracı olarak kullanılabileceğini gösteren ilk uygulama American Express ve Twitter işbirliği ile sunulan Amex Sync ürünüdür. Kişilerin Twitter hesaplarıyla American Express özellikli kartlarını eşleştirmesinin ardından aktif hale gelen bu sistemde, gönderilen bir "tweet" ile ürün satın alabilme kolaylığı sunulmak istenmiştir. Bunun için, Twitter servisi üzerinden atılan mesajın özel bir "hashtag" içermesi gerekmekte, ardından da kullanıcıdan yapmak istediği alım işlemi için onay vermesi beklenmektedir. Kullanıcının Twitter hesabının kontrolünü elinde bulundurduğu varsayımıyla, olağandışı bir işlem gerçekleştirildiğinde kullanıcı uyarılmaktadır. Ayrıca, satın alınan ürün sadece kişinin American Express hesabında ön tanımlı olan adresine gönderilebildiği için, farklı bir adrese gönderilme ihtimali/tehlikesi bulunmamaktadır. Ancak kişinin ödeme bilgileri Twitter hesabına bağlandığından, Twitter hesabının güvenliğini sağlamak bireyler için daha da önem kazanmaktadır. Bunun haricinde sosyal medya kullanılan mobil ödeme uygulamalarına örnek olarak PayPal' ın geliştirdiği Venmo uygulaması, Apple Pay üzerinden kullanıcıların mesajlaşma ile ödeme işlemleri yapabilmesi, Amerikan Bankaları ve kredi birlikleri tarafından küçük miktarlarda ödeme yapılabilen Zelle uygulaması, Facebook Messenger uygulaması verilebilir. Çin'de yaygın olarak kullanılan Tencent's WeChat and Alibaba's Alipay uygulamaları da sosyal medya ödeme yöntemleri olarak ortaya çıkmaktadır. Ancak ödeme bilgilerinin sosyal medya üzerinden paylaşılması hassasiyeti kullanıcıları bu tarz ödemelerden alıkoyan en önemli unsur olarak gözükmektedir. Avrupa, Afrika ve Latin Amerika'da faaliyet gösteren Accenture Payment Services'e göre tüketicilerin % 92'si finansal bilgilerini özellikle güvenlik endişesi nedeniyle, sosyal medya şirketleri ile paylaşma konusunda isteksizdir (BBC, 2017).

4. Mobil Ödemelerde Güvenlik ve Öneriler

Mobil ödeme sistemleri, bilgi sistemleri güvenliği açısından ele alındığında geleneksel kredi kartlı ödemelere göre daha fazla güvenlik riski taşımaktadır. Mobil ödeme sistemlerinde iletişimde hava ortamını kullanması, mobil cihazların kolaylıkla

ele geçirilebilir ve tekrar kullanılabilir olması ve mobil işletim sistemlerinin güvenlik unsurlarının kısıtlı olması mobil sistemleri dolandırıcılığa daha fazla müsait hale getirmektedir. Bu durum birçok saldırı için açık kapı bırakarak güvenlik açığı oluşturmakta ve karşı önlemler alınmazsa sistem güvensiz olmaktadır.

Mobil ödeme güvenlik unsurları dikkate alınarak bu bölümde, verinin saklanması ve iletişim esnasında ödeme sistemlerinde oluşan riskler, saldırı türleri ve çözüm önerileri ele alınmaktadır.

4.1. Verinin Saklanması Sırasındaki Güvenlik Riskleri ve Öneriler

4.1.1. Mobil Ödeme Cihazı (Güvenli Unsur)

1. Kullanıcı Hatası ve Dikkatsizlik: Ödeme uygulamasının ve hesap bilgisinin mobil cihaz içerisinde yer alması halinde, söz konusu veri sadece güvenli unsur içerisinde tutulmalı, başka bir yerde bulundurulmamalıdır. Bu durumda, ödeme verisi kullanıcının kontrolündeki mobil telefonda olduğundan dolayı, kullanıcı hata veya dikkatsizlerinden kaynaklanan riskler de değerlendirilmelidir. Söz konusu riske karşı alınabilecek yegâne önlem kullanıcıların bilgilendirilerek, farkındalıklarının artırılmasıdır.

2. Hassas Verilere Yetersiz Erişim Kontrolü Uygulanması: Mobil cihaza giriş yapılması esnasında yetersiz erişim kontrolü ve kimlik doğrulama kullanılması halinde ve kişisel veri hırsızlığı ve sahte işlem yapılması riskleri oluşacaktır. Söz konusu risklere karşı biri bilinen diğeri sahip olunan olmak üzere en az 2 faktörlü erişim yapılması veya erişimde biyometrik veri kullanılması da mobil cihazın güvenliği artırmaktadır.

Ayrıca, SIM karta erişim için zayıf parola kullanılması halinde SIM kartın kurcalanması veya klonlanması zafiyeti ve bunun sonucunda hassas ödeme verisi hırsızlığı ve kullanıcı yerine yasadışı finansal işlem yapılması riskleri oluşacaktır. Bu riskler söz konu olduğu durumlarda; SIM kart için güvenlik duvarı kullanımı, SMS PIN kullanılması ve yeterli anahtar uzunluğuna sahip gelişmiş şifreleme tekniği kullanılmasının uygun olacağı düşünülmektedir.

3. Hassas Verinin Güvensiz Saklanması: Mobil cihaz içerisinde hesap bilgisi ve ödeme uygulaması güvenli bir şekilde saklanmazsa bu verilerin elde edilmesi riski oluşacaktır. Bu nedenle, çok katmanlı güvenlik yaklaşımı güvenliğin sağlanmasında yardımcı olacaktır. Bu amaçla, farklı uygulamalar birbirinden bağımsız ve güvenli bir şekilde çalışmalıdır.

Güvenli unsur içerisinde farklı yetki ve doğrulama mekanizmaları ile çalışan birden fazla güvenlik alanı tanımlanmalıdır. Bunun için bir adet ihraççı güvenlik alanı (ISD-Issuer Security Domain), bir adet kontrol otoritesi güvenlik alanı (CASD- Controlling Authority Security Domain) ve farklı servis sağlayıcılar (kredi kartı, ön ödemeli kart, sadakat kartı, v.b.) için birden fazla ek güvenlik alanı (SSD- Supplemental Security Domain) tanımlanmalıdır (Smart Card Alliance, 2009).

ISD üretim aşamasında üretici tarafından oluşturulan kart içeriği güvenli bir şekilde elektronik haberleşme işletmecisine (MNO/ISP) iletilmelidir. Yeni bir ek güvenlik alanı için farklı yetkilendirilmeler yapılmalı ve her ek güvenlik alanı kendi güvenlik alanı oluşturulması ve yetkilendirilmesi ISD tarafından izin verilerek yapılmalıdır (Smart Card Alliance, 2009).

Ayrıca, güvenli unsurun SIM kart gibi bir çip içerisinde saklandığı durumlarda, fiziksel güvenlik önlemi olarak çipin termal ve UV (Ultra Violet – Morötesi) ışıkları ile yapılabilecek ataklara karşı ekstra bir metal katman içerisinde yer alacak şekilde üretilmiş olması gerekmektedir.

4. Zararlı Yazılımlar: Mobil cihazlara yanlışlıkla yüklenen zararlı yazılımlar, kimlik doğrulama verisinin yüklenen yazılımca ele geçirilmesi zafiyeti ve sonucunda doğrulama verisi kaybı, veri hırsızlığı ve işlemin reddedilmesi risklerini oluşturmaktadır. Kötü amaçlı yazılım, onaylanmış bir cihazdan kaynaklanan kullanıcı aktiviteleri sonucunda bir mobil cihazı istila edebilir ancak zarar verme potansiyeli, mobil cihazın root /jailbreak (Android/IOS işletim sistemli cihazlarda en yetkili kullanıcı olma) yapılması ve güvenilir olmayan kaynaklardan bir başka deyişle uygulama marketleri dışından yüklenen uygulamalarla önemli ölçüde artar. Zararlı yazılımların mobil telefonlardaki çalışma mekanizmaları bilgisayar ortamına benzemekle beraber, mobil telefonun bilgisayara göre daha kişisel olması sebebiyle (konum, entegre kamera, sürekli müşteri yanında olma, vb.) verebileceği zarar daha fazladır. Ek olarak, bilgisayar ortamındaki güvenlik kontrolleri olan antivirüs, güvenlik duvarı ve şifreleme, mobil ekosistemde henüz kabul edilebilir olgunluğa ulaşamamıştır.

Bu kapsamda, müşterilerin mobil telefonun uygun ve güvenli kullanımı hususunda bilinçlendirilmesi önem arz etmektedir. Güçlü parolaların önemi, güçlü parolaların yapısı, işletim sistemi ve uygulamaların güncellenmesinin önemi, jailbreak veya root edilmiş telefonun potansiyel sakıncaları, mevcut güvenlik uygulamaları, kimlik doğrulama verilerinin şifresiz biçimde telefonda saklanmasının potansiyel zararları, uygulamaları sadece güvenilen kaynaklardan indirmenin önemi gibi hususlarda müşterilerin bilgilendirilmesi önemlidir.

Bunun yanı sıra, güvenlik güncellemelerinden kaçınmak veya geciktirmek, bir cihazı güvenlik açıkları için kolay bir hedef haline getirmektedir. Söz konusu riskleri önlemek için yazılım yükleme için ekstra bir doğrulama mekanizması kullanılması, mobil cihazların root/jailbreak yapılmaması ve cihazlarda anti virüs ve zararlı yazılım engelleyici program kullanılması uygun olacaktır.

5. Mobil Cihaz Değiştirilmesi/Yenilenmesi: Mobil cihazların değiştirilmesi veya yenilenmesi esnasında güvenli unsur içerisinde yer alan uygulamaların yüklenmesi özellikle teknolojiye çok aşina olmayan kullanıcılar için konfigürasyon ve kurulum karmaşıklığı yaratmaktadır. Bu durum uygulamanın hatalı ve yetersiz güvenlikte kurulumu sonucunu doğurmaktadır. Önlem olarak uygulama yüklenmesi aşamasında kullanıcı etkileşiminin azaltılması gerekmektedir.

6. Yetersiz DRM Koruması: Mobil cihazda yetersiz dijital haklar koruması (DRM) kullanılması yasadışı içerik dağıtımı, içerik hırsızlığı, dijital korsanlık, dijital hak ihlali ve içerik sağlayıcı veya üye işyeri kazanç kaybına yol açmaktadır. Söz konusu risklerin önlenmesi için mobil cihazlarda şifre destekli DRM kullanılması uygun olacaktır.

4.1.2. Bulut

Ödeme verisinin bulutta tutulması durumunda, ödeme verisinin güvenliğinin bulut hizmetini veren paydaş tarafından sağlanması gerekmektedir. Böylece kullanıcının hata ve dikkatsizliklerinden oluşabilecek güvenlik riskleri minimize edilmektedir. Öte yandan, ödeme bilgilerinin kullanıcının sahip olduğu cihazdan başka bir yerde tutulması, kullanıcılarda güven problemi oluşturabilecektir.

Hassas ödeme verisinin saklandığı ortam, asgari olarak verinin kullanımı, korunması, saklanması, provizyonu ve iletimi konuları için geliştirilmiş bir standart olan Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi (Payment Card Industry -PCI-Security Standards Council) tarafından yayımlanan Veri Güvenliği Standardının (Data Security Standard – DSS) güncel versiyonunun gereklerini, tanımlanmış olan süre çerçevesinde yerine getirmelidir. PCI-DSS; 6 ana kriter altında tanımlanan 12 temel maddeden oluşmaktadır:

Bu kapsamda;

1. Güvenli ve sürekli bir ağ alt yapısı kurmak: Kart bilgilerini korumak için güvenlik duvarı konumlandırılması ve yapılandırılması, sistemde yer alan hiçbir yazılım ve donanımda ön tanımlı parolanın kullanılmaması,

2. Kart sahibinin bilgilerini korumak: Kart bilgilerinin güvenli şekilde saklanması, genel ağlarda kart bilgilerinin şifreli olarak gönderilmesi,

3. Güvenlik açığı yönetimi oluşturmak: Düzenli olarak güvenlik yazılımlarının güncellenmesi, güvenli sistem ve uygulama geliştirilmesi, geliştirmenin süreklilik arz etmesi,

4. Etkin erişim kontrolü uygulamak: İşletme tarafında kart bilgilerine erişim kısıtlamasının getirilmesi, her kullanıcının kendine ait bir kullanıcı hesabının olması ve oturumu bu kullanıcı hesabı ile açması, kart bilgilerine erişimin fiziksel olarak engellenmesi,

5. Düzenli olarak izlemek ve test etmek: Kart bilgilerine ve ağa gelen tüm erişimlerin izlenmesi, güvenlik sistemleri ve süreçlerin devamlı olarak test edilmesi,

6. Bilgi güvenliği politikası uygulamak: Tüm personel için bilgi güvenliğini ilgilendiren sürdürülebilir bir politikanın uygulanması kriterleri uygulanmalıdır.

Bunlara ek olarak, hassas ödeme verisinin üye işyerine hiç iletilmemesi gerekmektedir. Ancak ödeme teyidinin yapılması için bir veri gönderilmesi gerekmesi halinde ise hesap numarası veya hassas ödeme verisi yerine her ödeme için oluşturulan farklı bir token iletilmeli ve daha sonraki ödemeler için oluşabilecek riskler ortadan kaldırılmalıdır.

4.2. Verinin İletilmesi Sırasındaki Güvenlik Riskleri ve Öneriler

Ödeme işlemi, üçüncü bölümde de belirtildiği gibi, NFC, QR Kodu, SIM/USSD ve/veya internet teknolojileri kullanılarak yapılabilmektedir. Gelişen teknolojilere paralel olarak, saldırganlar her geçen gün kendilerini geliştirmekte ve yeni metotlara başvurmaktadır. Mobil uygulama kullanımının yaygınlaşması nedeniyle tek bir mobil cihaz içerisinde, kişisel veriler, kişisel finansal uygulamalar, sosyal medya uygulamaları ve kurumsal uygulamalar da bir arada bulunmakta ve bu durum saldırı yüzeylerini artırmaktadır. (Isaac ve Zeadally, 2014.)

Bu bölümde veri iletişimine yönelik genel riskler ve önlemler tartışılacak sonrasında bilinen saldırı türleri ve alınabilecek önlemler hakkında bilgi verilecektir. Bölümün sonunda ise her iletişim tekniğine özel zafiyetler, riskler ve alınabilecek önlemler ele alınacaktır.

1. **POS ile Cihaz arasında Hava Yoluyla İletişim (Over the air- OTA):** Veri iletiminin hava yolu ile yapılması trafiğin birbiri ile karışması ve sonu-

cunda Replay (Tekrarlama) saldırısı, veri hırsızlığı veri değiştirilmesi risklerini oluşturmaktadır. Bu risklere karşı veri iletimi için güvenli protokol ve güvenilir platform modülleri (TPM) kullanılması ve veri iletiminin şifreli olarak yapılması önlemleri alınabilir.

2. **Üye işyerinde kurulu POS cihazları:** POS cihazlarının fiziksel olarak üye işyerinde bulundurulması sahtecilik saldırıları ve POS cihazının kurcalanması ve sonucunda ödeme işleminin yetkisiz yere yönlendirilmesi, Replay Saldırısı risklerini oluşturmaktadır. Karşı önlem olarak, periyodik POS testi yapılması ve ödeme işlemi için mesaj doğrulaması yapılması gerekmektedir.

3. **Akıllı telefon internet ve GPS yetenekleri:** Akıllı telefonların sahip olduğu internet ve GPS yetenekleri, mobil cihazlara zararlı yazılımlar yüklenmesi, veri değiştirilmesi, kullanıcı davranışının belirlenmesi ve mesaj değiştirilmesi riskleri oluşturmaktadır. Bu risklere karşı konum servislerinin kullanıcı kontrolünde olması, iletişimin şifreli yapılması ve güvenilir platform modülleri (TPM) kullanılması önlemleri alınmalıdır.

4. **GSM Protokolünden Kaynaklanan Sorunlar:** GSM protokolünde yer alan şifreleme zayıflıkları (şifresiz SMS gönderimi), gönderilen SMS mesajının değiştirilmesi, Replay saldırısı, içerik ve servisin çalınması ve yasadışı fon transferi riskleri oluşturmaktadır. Karşı önlem olarak, güçlü şifreleme protokolleri kullanımı, SMS mesaj doğrulaması yapılması alınmalıdır.

   Bunun yanı sıra, GSM protokolünde karşılıklı doğrulama eksikliği ise mesajın içeriğini bozma, değiştirme, man in the middle (araya girme) atakları, dinleme ve Replay Saldırılarına yol açmaktadır. Bu nedenle, mesajların karşılıklı olarak doğrulanması için bir mekanizma oluşturulmalıdır.

5. **Zayıf Şifreleme Algoritmaları ve Anahtarı Kullanımı:** Zayıf şifreleme algoritmaları ve anahtarları, şifreleme analizi yapılması, sözlük atakları, kısıtlı fonksiyonlara yetkisiz erişim yapılması risklerini oluşturmaktadır. Söz konusu risklere karşı, yeterli anahtar uzunluğuna sahip gelişmiş şifreleme tekniği kullanılması ve tahmin edilemez şifre kullanılması uygun olacaktır.

4.2.1. Veri İletişimine Yönelik Saldırılar

Mobil ödeme sistemlerinde kullanılan iletişim teknolojilerine yönelik bilinen saldırılar şunlardır:

Dinleme (Eavesdropping):

Mobil ödemelerde veri iletişimi kablosuz olarak yapıldığı için iletişimin üçüncü şahısların dinlemesine açık olduğu aşikârdır. İki cihaz iletişime geçtiği zaman aralarında sinyal trafiği belirli bir yakınlığa yerleştirilen uygun bir dinleme cihazı ile dinlenebilmektedir.

İletişim için internet teknolojisinin kullanıldığı mobil ödemelerde, şifresiz olarak gerçekleşen veri iletişimi, dinleme saldırılarına açık bir ortam sağlamaktadır. SMS kullanılarak yapılan ödemelerde ise her ne kadar mobil telefon ile baz istasyonu arasındaki iletişim şifreli olsa da, baz istasyonundan sonra operatörün ağına kadar olan trafik şifresiz yapıldığı için dinleme saldırılarına elverişli bir ortam ortaya çıkmaktadır. Ancak, NFC ve QR kod kullanılarak yapılan mobil ödemelerde veri iletişimi çok kısa mesafelerde yapıldığı (yaklaşık 10 cm) ve iletişimde çok düşük güçte sinyaller kullanıldığı için dinleme yapılması diğer teknolojilere göre daha zordur.

Ayrıca iletişimin dinlenmesi fiziksel (sinyalinin gücü, kullanılan antenin türü ve geometrisi, kullanılan alıcının ve şifre çözücünün (decoder) türü ve kalitesi v.b.) ve çevresel (saldırganın pozisyonu, yeri ve ortamdaki gürültü) birçok etkene bağlı olması nedeniyle çok kolay olmadığı sonucuna varılmaktadır (Haselsteiner ve Klemens, 2006). Bunun yanı sıra dinleme, cihazın aktif ya da pasif modda çalışmasına göre farklılık göstermektedir. Pasif modda cihaz, aktif cihazın oluşturduğu elektromanyetik alan tarafından harekete geçirildiği için dinleme yapılması daha zordur (Van Damme ve Karel, 2009).

Veri Bozulması:

Veri bozulması saldırılarında, saldırgan sadece iletişimi dinlemekle kalmaz iletişimin bozulmasına sebep olur. Mantık olarak servis durdurma (DOS) saldırılarına benzemektedir. Bu saldırı türünde veri değiştirilmemekte, sadece bozularak iletişim engellenmektedir.

Söz konusu saldırı QR kod kullanılan iletişimlerde uygulanabilir değildir. İnternet yoluyla yapılan mobil ödemelerde veri bozulması mümkün olmakla birlikte, TCP/IP protokolünün doğasından kaynaklanan üç aşamalı el sıkışma mekanizması nedeniyle verinin bozulduğu tespit edilip tekrar doğru verinin gönderilmesi sağlanabilmektedir. SMS/USSD kullanılarak yapılan ödemelerde ise verinin bozulmasına elverişli bir ortam sağlanmaktadır.

İletişim için NFC teknolojisinin kullanıldığı durumlarda veri bozulması saldırıla-

rı, doğru zamanda doğru frekansta sinyalin iletişim ortamına gönderilmesi yoluyla yapılır. İletişimde kullanılan modülasyon ve kodlama tekniği bilinirse sinyalin hangi zamanda gönderileceği hesaplanabilmektedir. Hesaplanan zamanda iletişimde kullanılan sinyalle aynı frekansta sinyal iletişim ortamına gönderilerek iki cihaz arasındaki iletişim bozulmuş olur. Saldırıyı gerçekleştirmek için kullanılacak sinyallerin gücü yüksek olduğu ve NFC cihazlar sinyal gönderirken mevcut RF alanı kontrol ettiği için iletişime geçen cihazlar tarafından kolaylıkla tespit edilebilmekte ancak önlenememektedir (Haselsteiner ve Klemens, 2006).

Veri Değiştirilmesi:

Veri değiştirilmesi saldırılarında, verinin saldırganın istediği şekilde değiştirilmesi amacı güdülmektedir. Veri bozulması saldırısı ile eşdeğer mekanizmalara ek olarak iletişime veri enjekte edilmesi gerekmektedir.

Söz konusu saldırı QR kodu, SMS/USSD ve internet kullanılan iletişimlerde, zararlı yazılımlardan faydalanılmaksızın uygulanamamaktadır. NFC' de ise veri iletişim hızı ve kullanılan kodlama tekniğine göre farklılık göstermektedir. NFCIP standardına göre veri değişikliği gerçekleşmesi, yüksek veri iletişim hızları için mümkünken, düşük veri iletişim hızlarında (106 KBaud) çok da ihtimal dâhilinde görülmemektedir (Van Damme ve Karel, 2009). 106 KBaud hızını ve aktif modu kullanmak veri değişimi saldırılarını önlemekte ancak iletişimi dinleme saldırılarına daha hassas hale getirmektedir. Buna ek olarak cihazların veri göndermeden önce RF alanı kontrol etmeleri, saldırıları tespit etmekte ancak önleyememektedir.

Araya Girme (Man-in-the-middle):

Bu saldırı türünde iletişime geçmek isteyen iki taraf da birbirleriyle güvenli iletişim yaptıklarını düşünürken, arada bir yerde konuşlanan saldırgan her ikisiyle de iletişime geçmektedir. Saldırgan, bir taraftan aldığı mesajı değiştirerek veya sadece dinleyerek diğer tarafa göndermektedir.

Söz konusu saldırı internet üzerinden şifresiz olarak gerçekleşen iletişimde uygulanabilmekle birlikte, şifreli gerçekleşen iletişimde uygulanamamaktadır. QR kodu ve NFC teknolojilerinin kullanıldığı ödemelerde çok yakın mesafelerden okuma yapıldığı için bu tarz ataklar için elverişli bir ortam oluşturmamaktadır. Ayrıca NFC teknolojisinde, araya girerek dinleme yapacak cihazın aynı anda sinyal alıp gönderiyor olabilmesinin gerekmesi problem oluşturmakta ve RF alanı cihazlar tarafından kontrol edilerek olası çarpışmalar tespit edilebilmektedir (Van Damme ve Karel, 2009).

Tekrarlama (Replay):

Bu saldırı türünde müşteri, işyerinde yer alan cihazın ekranında yazan değer kadar ödediğini düşünerek ödemeyi gerçekleştirmektedir. Bu aşamadan sonra aynı ödeme bilgisi kullanılarak onay verilmiş olan miktardan çok daha büyük miktarlarda ödeme işlemi gerçekleştirilmektedir. Söz konusu saldırıda kullanılan, üzerinde oynama yapılmış sahte bir POS cihazı ile üye işyeri anlaşması yapan kuruluşa bağlanmak mümkün olmasa da, oynama yapılmamış asıl POS cihazına bağlanmak mümkündür. Saldırganın müşterinin önüne getirdiği cihaz, sahte bir POS cihazı olup kablosuz ağ üzerinden yakınlardaki bir suç ortağı ile veri alışverişi yapmaktadır. Müşteri bu durumdan habersiz bir şekilde ödemeyi gerçekleştirdiğinde, hesabından onay verdiğinden daha fazla bir meblağ çıkmış olmaktadır.

Bu duruma özel olarak iki çözüm önerisinde bulunulabilir. İlki alışveriş sonrası müşterinin mobil telefonuna, mobil ödeme hizmet sağlayıcının, alışverişe ilişkin bilgileri iletmesidir. İkinci çözüm önerisi de POS cihazı ile mobil ödeme aracı arasında geçen haberleşme süresine kısıt konulmasıdır. Sonuçta ödeme sistemi ile okuyucu arasına bir mesafe girmektedir ve haberleşme zaman almaktadır.

4.3. NFC

NFC ödemeler güvenli, hızlı ve kullanışlı olmasından dolayı giderek yaygınlaşmaktadır. Bunun yanı sıra mobil cihazların kullanımının artmasıyla birlikte NFC kullanımı da giderek artmaktadır. NFC ödemeleri, işlemde kullanılan verilerin şifreli ve dinamik olması yani sürekli değişmesi nedeniyle manyetik şeritli bir kartın arka tarafında yer alan ve ödemede kullanılan statik verilere karşıt olarak daha fazla güvenlik sunmaktadır. NFC ödemelerde hassas ödeme verileri, sahtekârlar için anlaşılmaz ve dolayısıyla kullanılamaz bir şekle dönüştürülmektedirler (tokenization). Bu tokenlar her NFC ödeme işleminde farklı olup, böylece bu bilgilerin ayrıştırılıp, elde edilmesi neredeyse imkânsız hale gelmektedir. Söz konusu gizliliği sağlamanın bir diğer yolu da, yukarıda tartışıldığı gibi iletişimi şifreli yapmaktır. Ancak bu durumda iletişimde yavaşlama olacağı aşikardır.

Örnek olarak Apple Pay, kullanırken kredi kartınızın resmini çekip telefona yükledikten sonra Apple kart bilgilerini kart ihraç eden kuruluşa gönderir. Bankalar, ödeme verilerini rastgele oluşturulmuş bir dizi sayı ile değiştirir (simge/token) ve bu rasgele sayı, Apple' a geri gönderilir, ardından telefona programlanır. Böylece telefondaki hesap detayları, saldırganlar tarafından kopyalanamaz. Bunun yanı sıra, Apple Pay, Apple'ın parmak izi teknolojisi olan Touch ID ile korunmaktadır. Bir Apple

Pay işlemini başlatmak için, telefonu parmak izi ile açmak gerekmektedir. Cihaz çalınsa bile, verilere ulaşılamayacaktır.

NFC ödeme sistemleri güvenli olmayan iletişim ortamı (hava) kullanıldığı ve ödemeyi yapan NFC cihaz ile POS arasındaki trafik fiziksel katmanda hiçbir kontrole tabi tutulmadığı için, iletişime geçen her iki cihazın da doğrulanması mümkün olmamaktadır. Bu durumda iletişim yapan iki cihazdan birinin yerine başka bir cihaz yerleştirilerek birçok verinin ele geçirilmesi veya yanlış sinyallerle POS ya da ödeme aracının devre dışı bırakılması (DOS) ataklarına karşı elverişli bir iletişim ortamı oluşmaktadır. Ayrıca ödeme sisteminin içerisinde yer alan işlem sayacı, kişisel doğrulama numarasının (PIN) yanlış girilmesi halinde sistemi devre dışı bırakmaktadır. Bu durumda mobil cihazın servis durdurmaya karşı savunmasız kaldığı aşikârdır.

İki cihaz arasında güvenli bir iletişim kanalı kurulması dinleme, bozma ve değiştirme saldırılarına karşı alınabilecek en güvenli önlem olarak düşünülebilir (Haselsteiner ve Klemens, 2006). Araya Girme saldırıları NFC protokolünün doğası gereği kapsamda olmadığından güvenli kanal oluşturulması doğrulama gerektirmeyen bir anahtar değişim mekanizması ile kurulabilir. Bu kapsamda, RSA ya da Elliptic Curves asimetrik kriptografik algoritmasına dayanan Diffie-Hellmann anahtar değişim mekanizması ile iki cihaz arasında gizli bir paylaşılan anahtar oluşturulur. Paylaşılan anahtar kullanılarak 3DES (Triple Data Encrypion Algorithm), AES (Advanced Encryption Standard) gibi simetrik anahtar oluşturulur ve bu anahtarla iletişim güvenli bir şekilde yapılır. Böylelikle iletişimde gizlilik, bütünlük ve doğrulama sağlanmış olur (Haselsteiner ve Klemens, 2006). Bunlara ek olarak, aktif-pasif iletişim kullanılması, veri gönderen cihazın RF alanı kontrol ederek saldırı varlığını tespit etmesi ve iki cihaz arasında güvenli bir kanal oluşturulması, olası saldırılara karşı güvenlik önlemi olarak alınmasının faydalı olacağı düşünülmektedir (Van Damme ve Karel, 2009).

NFC ödemelerde mobil cüzdan kullanıldığında daha fazla güvenlik için, kullanıcı mobil cüzdan uygulamasını kendi cihazında açtığında, mobil cüzdan yalnızca NFC okuyucuları ile iletişim kurar, kullanılacak ödeme kartını seçer ve ödeme işlemini tamamlar. Başka bir güvenlik önlemi de NFC ödeme okuyucularının bir seferde yalnızca bir NFC ödeme cihazına bağlanmasıdır. Böylece, yakındaki bir müşterinin yanlışlıkla başka bir satın alma işlemi için ödeme yapma tehlikesinin önüne geçilmiş olur. Son olarak, alınabilecek genel bir önlem müşterinin harcama alışkanlıklarının izlenmesidir. Saldırganlar genelde kolay nakde çevrilebilen pahalı ürünler almaya meyilli olduğundan müşterinin normal harcama alışkanlıklarının dışına çıktığı ödemeler tespit edilebilmekte ve müşteriler uyarılarak saldırıların önüne geçilebilmektedir.

4.4. QR Kodu

Bir QR kodu taranmadan, içerisindeki verinin vaat ettiği yere mi, yoksa zararlı bir web sitesine veya uygulamaya mı yönlendireceği görsel olarak anlaşılamaz. Bu sebeple, müşterinin ödeme amacıyla işyeri tarafından üretilen QR kodunu mobil telefonuna okutması durumunda, mobil telefona sahte bilgiler içeren QR kodu okutulması en büyük güvenlik açığı olarak düşünülebilir. QR kodun bizzat mobil ödeme uygulaması tarafından okunması, QR kodunun işyerinin kimliğinin doğrulanmasına yönelik kriptografik teknikleri içermesi ve ödeme işleminin QR kodu okunmasına müteakip müşterinin onayı neticesinde gerçekleşmesi söz konusu güvenlik riskini azaltacaktır.

QR kodu ile ödeme metotlarından ikincisi olan, bir QR kodun müşteri tarafından mobil telefona okutulması ile telefonun bir internet sayfasına yönlendirilmesi sonrasında müşterinin alışveriş yapıp ödeme gerçekleştirmesi durumu oldukça risklidir. QR kodlarının güvenliği noktasında bilinmesi gerekenler, bu kodları üretmenin ne kadar kolay olduğu ve içine hangi bilgilerin sıkıştırılabileceğidir. Web adresi, konum bilgileri, SMS mesajı, kablosuz ağ giriş bilgileri, PayPal "Hemen Öde" linki gibi onlarca veriyi bir QR kodunun içine sığdırmak mümkündür. Bu kolaylık nedeniyle, virüsler, casus ve kötü amaçlı yazılımlar da QR kodlarıyla birlikte yayılmak için kendilerine yeni bir mecra bulmuşlardır. Bu noktada, içeriğe doğrudan erişen QR kod tarayıcı uygulamalar yerine ("run first, ask questions later"), yönlendirmeden önce içerik hakkında bilgi veren uygulamaları kullanmak tavsiye edilmekte ancak yeterli olmamaktadır. TinyURL, bitly ve goo.gl gibi URL kısaltma servisleri kullanıldığında yönlendirilecek içerik perdelenmekte ve kaynağı bilinememektedir. Ayrıca, mobil cihazlarda anti-virüs yazılımı, güvenlik duvarı gibi güvenlik sağlayıcı uygulamaların kullanımının yaygın olmadığı görülmektedir. Dolayısıyla kullanıcılar, kaynağından emin olmadıkları bir QR kodunu tarayıp çalıştırmanın, taşıdığı riskler hakkında bilgilendirilmelidir. Bu sebeplerle bu tip QR kodu kullanımları güvenlik açısından uygun görülmemektedir.

Mobil telefonda oluşturulan QR kodunun işyerine ait olan okuyucu cihaza okutulması durumunda, işyerinin QR kod ile iletilen veriyi kaydetmesi riski mevcuttur. Bu sebeple, hiçbir durumda işyerine hassas ödeme verisi iletilmemelidir. Bunun yerine mobil ödeme hizmet sağlayıcının müşterinin kimliğini doğrulamada kullanacağı ve rastgele üretilen bir jeton mahiyetinde olup hiçbir anlamlı veri içermeyen QR kodu kullanılmalıdır. Kullanıcı tarafında, uygulama içerisinde üretilen QR kodunun güvenliğini sağlamak son derece önemli olduğundan, güçlü bir parola/PIN kullanılması tavsiye edilmektedir. Ayrıca mobil ödeme uygulaması, her alışverişte ya da müşteri talebi halinde kullanılan QR kodunu değiştirmelidir. Bunlara ek olarak müşteriye ile-

tilecek bir teyit mesajını müşterinin onaylayarak ödeme işlemini doğrulaması veya müşteriye ödemeye ilişkin bir bilgilendirme mesajının iletilmesi güvenlik açısından riski azaltacak diğer etkenlerdir.

Bunlara ek olarak, kullanıcıların düzenli aralıklarla bilgilendirilerek farkındalığın artırılması da söz konusu güvenlik riskini ortadan kaldırmak için önemlidir. Mobil cihazını ödeme aracı olarak kullanan bir kişi, telefonunun ele geçirilmesinin cüzdanını kaybetmekle eşdeğer olabileceği düşünerek, öncelikle cihazının güvenliğini sağlamalıdır. Bu noktada, mümkün olan durumlarda verilerinin erişimini bir şifre ile korumalı, güvenmediği kaynaklarla paylaşılan kişisel bilgilerini sınırlandırmalıdır. İşyeri tarafında ise alınabilecek önlemlerden biri, taranılan QR kodunun, akıllı cihazı nereye yönlendireceği konusunda müşterilerin bilgilendirilmesidir. Örneğin, işyerinin sunduğu QR kodunun kendisini bir mobil kupona yönlendirmesi gerektiğini bilen bir kullanıcı, bu noktada hassas bilgilerini girmeyecektir. İşyerinin alabileceği diğer bir önlem ise domain adının mümkün olduğunca kısa olması ve kullanıcının URL'ı tümüyle görebilmesinin sağlanmasıdır. Buna ek olarak URL kısaltmalarının uzun halini görmeye yarayan "unshorten.me" gibi internet servislerden de faydalanılabilir.

4.5. SMS/USSD

SMS ve USSD, GSM şebekesi üzerinden veri aktarmak için kullanılan protokollerdir. Yapısal olarak mobil telefon ile baz istasyonu arasındaki radyo bağlantısı şifrelenmekle birlikte, baz istasyonundan itibaren şifresiz olarak iletilebilmektedir. Bu nedenle iletim esnasında söz konusu mesaj veya kodlar saldırıya açıktır. Söz konusu güvenlik açığının giderilmesi için mobil ödeme için kullanılan SMS/USSD kodlarının her aşamada şifreli olarak iletilmesi gerekmektedir.

Mobil ödeme sistemlerinde SMS kullanıldığında kullanıcıya ait hassas veriler ve ödeme verileri bir süreliğine de olsa mobil ağ operatörünün kontrolündeki ortamlarda bulunmaktadır. GSM operatörü bünyesinde geçici olarak tutulan mesajlara ilişkin normal mesajlara göre daha fazla güvenlik önlemi alınması gerekmektedir. Bu mesajların kısa süreli de olsa operatör tarafından şifreli olarak tutulması iyi bir karşı önlem olacaktır. USSD kodlarında ise böyle bir problem mevcut değildir. USSD kodları çevrimiçi çalışmakta ve hassas veri transferi bir yerde depolanmadan gerçekleşmektedir. USSD kodlarında da kullanıcı müdahil olmadan bazı kodlarla mobil cihazlarda değişiklik yapılabilmesi sorunu mobil ödemeler için üzerinde durulması gereken bir açıklıktır. Kullanıcı müdahil olmadan mobil cihazlarda gerçekleşen bu değişiklikler mobil cihaz içerisinde yer alan verilerin çalınması ya da silinmesi gibi noktalara gelebilmektedir. Bu durum saldırganlar için geniş bir hareket alanı oluşturmakta

ve işletim sisteminden kaynaklanan açıklıklar ciddi güvenlik açığı teşkil etmektedir. Bu nedenle özellikle ödeme işlemlerinde kullanıcı onayı olmadan USSD kodları vasıtasıyla bir işlem yapılmaması gerekmektedir.

Yukarıda sayılanlara ek olarak, bazı akıllı telefon işletim sistemlerinde otomatik olarak yüksek ücretli SMS atan, finans kuruluşlarından gelen SMS' leri engelleyip başka bir numaraya ileten zararlı yazılımlar mevcuttur. Bu başlık altında önerilen güvenlik önlemleri, açıkları kapatmakta yeterli olmamakta veya sistemin doğası gereği açıklar kapatılamamaktadır. Bu çerçevede USSD metodunun bütün mobil ödemelerde, SMS metodunun ise orta veya yüksek düzeyde risk taşıyan mobil ödemelerde kullanılması güvenlik açısından uygun görülmemektedir (Pegueros, 2012).

4.6. İnternet

İnternet üzerinden yapılan mobil ödemelerde müşterileri tanımlamak ve müşterilerin kimliğini doğrulamak için kullanılan bütün hassas ödeme verileri; saklanırken, işlenirken ve aktarılırken korunmalıdır. Söz konusu veriler internet üzerinde iletilirken, iletişim kuran taraflar arasında uçtan uca şifrelenerek veya simgeleştirilerek (tokenization) aktarılmalıdır.

Ayrıca kullanıcı doğrulamasının güvenli bir şekilde yapılması, oluşabilecek riskleri en aza indirmek için önem arz eden bir diğer konu olarak ele alınabilir. Kimlik doğrulama için karşılıklı kimlik doğrulama teknikleri kullanılmalıdır. Karşılıklı kimlik doğrulamada ödeme kuruluşu tarafından müşterinin/işyerinin kimliği doğrulanırken aynı zamanda müşteri/işyeri tarafından ödeme kuruluşunun kimliğinin doğrulanması gerçekleşir. Bu husus SSL/TLS protokolleri kullanılarak sağlanılabilir. Kullanılacak sertifikanın, genel kabul görmüş ve endüstri standardı haline gelmiş bir sertifika otoritesi tarafından imzalanması müşteride/işyerinde oluşacak güveni arttıracaktır. Bunun yanı sıra başarısız oturum açma girişimleri belli bir sayıyla sınırlanmalı ve bir oturum belli bir süre boyunca kullanılmadığında sonlandırılmalıdır.

Son olarak ödeme işleminin sosyal ağlar üzerinde yapılması hassasiyet arz eden bir diğer konu olarak düşünülebilir. Bu durumda alınabilecek güvenlik önlemleri internet üzerinde kullanılması haline göre daha sıkı olmalıdır. Bu noktada en önemli husus sosyal medya hesabına girerken çift faktörlü veya çift kanallı doğrulama kullanılması gerekliliğidir. Bunun yanı sıra sosyal medya üzerinden ödeme işlemleri yapılırken kart bilgilerinin her işlem esnasında tekrar girilmesi, PIN kullanılması ya da parmak izi ve benzeri metotlarla kullanıcı kontrolünden gerçekleştirilmesi sağlanmalıdır. Genel güvenlik prensipleri olarak nitelendirilebilecek uzun ve karmaşık şifre kullanımı, şifrenin belirli periyotlarda değiştirilmesi ve farklı sosyal medya hesaplarında farklı şifreler kullanılması, kullanıcı adı ve şifrelerin başkalarıyla paylaşılmaması,

kullanıcı adı olarak birebir aynı kişisel bilgilerin kullanılmaması, sosyal mühendisliğe karşı dikkatli olunması yani bilinmedik e-postalardaki linklere tıklanılmaması ya da eklentilerin açılmaması, ödeme işlemlerinin halka açık kablosuz ağlar üzerinden gerçekleştirilmemesi gerekmektedir.

5. Sonuç

Mobil ödeme sistemleri, mobil cihazlar kullanılarak başlatılan, yetkilendirilen veya onaylanan ödemeler olarak tanımlanabilmektedir. Mobil ödemeler işyerlerine, müşterilerin konum, alışveriş alışkanlıkları ve tercihleri bilgilerini kullanarak daha kişiye özel ve kaliteli hizmet verme imkânını sunmaktadır. Müşterilere ise, ürünlerin farklı yerlerdeki fiyatına, indirimlere ve diğer kampanyalara ait bilgiye erişim ve kıyaslama kolaylığı sunarak daha etkin kullanım sağlamaktadır. Bu avantajlarının yanında mobil ödemeler, birçok tehdit ve güvenlik sorunuyla karşı karşıyadır.

Bu çalışmada özetle mevcut mobil ödeme sistemleri incelenmiş, sınıflandırılmış, paydaşlar tanımlanmış ve güvenlik için alınması gereken önlemler üzerinde durulmuştur. Farklı mobil ödeme araçlarının farklı güvenlik gereksinimleri olabilmektedir. Bu sebeple güvenlik perspektifinden, ortak güvenlik gereksinimleri olan ödeme mekanizmaları gruplanmıştır. Bu gruplama ödeme verisinin saklandığı yere göre ve ödeme işleminde kullanılan iletişim teknolojisine göre gerçekleştirilmiştir.

Bu kapsamda, ödeme verisinin güvenli unsur içerisinde saklanması halinde de ekstra güvenlik önlemleri alınması, bulut ödemelerde ise ödeme teyidinin hesap numarası veya hassas ödeme verisi yerine farklı bir dinamik unsurla (token v.b.) yapılması gerektiği sonucuna ulaşılmıştır.

Ödeme için NFC kullanılması halinde, mobil cihazın pasif modda çalıştırılması, veri göndermeden önce RF alanını kontrol etmesi, ödeme işlemi bilgisinin kullanıcının mobil cihazına iletilmesi, mobil cihazla POS cihazı arasındaki haberleşme süresine kısıt konulması, güvenilir olmayan kaynaklardan uygulama indirmenin zararları hakkında kullanıcı farkındalığının artırılması ve uygulamalar için ekstra bir güvenlik katmanın kullanılması (parmak izi, PIN, yüz tanıma) önerilmektedir. Ödeme için QR kodu kullanılması halinde, her alışverişte değişken bir kod kullanılması, URL yönlendirilmesinin işyeri tarafından yapılması ve domain adının kısa olması sonuçlarına ulaşılmıştır. Bunlara ek olarak, USSD metodunun hiçbir ödeme işleminde kullanılmaması, SMS metodunun ise orta ve yüksek düzeyde risk taşıyan mobil ödemelerde kullanılmaması tavsiye edilmektedir. Son olarak, internet ödemelerinde SSL ve/veya TLS gibi güvenli protokollerin kullanılması, sosyal medya üzerinden yapılan ödemelerde çift faktörlü ve çift kanallı doğrulama yapılmasının uygun olacağı düşünülmektedir.

Kaynakça

1. Ashay, S. J. ve Joon S. P.. (2016). A Security Analysis on Apple Pay. 2016 European Intelligence and Security Informatics Conference, s. 160-163

2. Aydın, G. ve Burnaz, Ş.. (2016). Mobil Cüzdan Kullanım Niyeti ve Kişisel Yenilikçiliğin Aracılık Etkisi. Finans Politik & Ekonomik Yorumlar 2016 Cilt: 53 Sayı: 611, s. 71-90.

3. Aygören, O. ve Varnali, K.. (2011). Value-Based Analysis of Mobile Tagging. International Journal of E-Business Research, Vol. 7, No.1, p.93-104.

4. BBC. (2017). 02.12.2018 tarihinde https://www.bbc.com/news/business-42237432 adresinden erişildi.

5. Berg Insight. (2017). http://www.berginsight.com/ReportPDF/ProductSheet/bi-pos3-ps.pdf sitesinden 27.11.2018 adresinden erişildi.

6. Bozkurt, F. ve Ergen, A.. (2011). Pazarlama İletişiminde Yeni Bir Mobil Pazarlama Aracı: 2 Boyutlu Barkodlar. 16. Ulusal Pazarlama Kongresi, İstanbul.

7. Carr, M. (2010). Mobile Payment Systems and Services: An Introduction. 26.12.2018 tarihinde http://www.academia.edu/2563249/Mobile_Payment_Systems_and_Services_An_Introduction adresinden erişildi.

8. Dahlberg, T., Mallat N., Ondrus, J. ve Zmijewska, A.. (2008). Past, Present and Future of Mobile Payments Research: A Literature Review. Journal of Commerce Research and Applications 7: 165–81.

9. Ghiron, S. L., Medaglia, C.M. ve Perrone, A.. (2009). Art-sonomy: Social Bookmarking of Real Artworks via Mobile Applications with Visual Tags. International Conference on Universal Access in Human-Computer Interaction, s. 375-384.

10. GlobalPlatform, The Standard For Secure Digital Services and Devices. (2018). Introduction to Secure Elements. 26.12.2018 tarihinde https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf adresinden erişildi.

11. Güven, V. ve Şahinöz, E.. (2016). Blokzincir Kripto Paralar Bitcoin Satoshi Dünyayı Değiştiriyor. Kronik Kitap.

12. Haselsteiner, E., ve Klemens, B.. (2006). Security in Near Field Communication (NFC). Graz: Workshop on RFID Security.

13. Hopi. (2018). 27.11.2018 tarihinde https://hopi.com.tr/ adresinden erişildi.

14. InvestingAnswers. (2019). 28.01.2019 tarihinde https://investinganswers.com/search/term/p2p adresinden erişildi.

15. Isaac, J.T. ve Zeadally, S.. (2014). Secure Mobile Payment Systems. IT Pro May/June 2014.

16. Kim, C., Mirusmonov, M. ve Lee I.. (2010). An Empirical Examination of Factors Influencing the Intention to Use Mobile Payment. Computers in Human Behavior 26(3), pp.310–22.

17. Linck, K., Pousttchi, K. ve Wiedemann, D.G.. (2007). Security Issues in Mobile Payment from the Customer Viewpoint. Proceedings of the 14th European Conference on Information Systems, pp.1–12

18. Murdoch, S. J., Drimer, S., Anderson, R. ve Bond, M.. (2010). Chip and PIN is Broken. IEEE Symposium on Security and Privacy.

19. Ondrus, J. ve Pigneur, Y.. (2006). Towards a Holistic Analysis of Mobile Payments: A Multiple Perspectives Approach. Electronic Commerce Research and Applications 5 (3), pp.246–57.

20. Pegueros, V. (2012). Security of Mobile Banking and Payments. 26.12.2018 tarihinde https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062 adresinden erişildi.

21. Smart Card Alliance. (2009). Security of Proximity Mobile Payments (White Paper). New Jersey: Smart Card Alliance.

22. Smart Card Alliance. (2011). The Mobile Payments and NFC Landscape: A U.S. Perspective A Smart Card Alliance Payments Council.

23. TBB (Türkiye Bankalar Birliği). (2011). Kayıtlı Ekonominin Geliştirilmesi Sürecinde Kartlı Ödeme Sistemleri ile Yeni Yöntem ve Teknolojiler. Vergi Konseyi, Yayın No: 274, İstanbul.

24. Tearsheet. (2018). 30.11.2018 tarihinde https://www.tearsheet.co/payments/what-mobile-payment-providers-can-learn-from-starbucks adresinden erişildi.

25. Van Damme, G., ve Karel, W.. (2009). Practical Experiences with NFC Security on Mobile Phones. Leuven: Workshop on RFID Security.

26. Varnali, K., Toker, A. ve Yılmaz, C.. (2011). Mobile Marketing Fundamentals and Strategy, McGraw Hill, 1st Edition.

27. Wang, Y., Hahn, C. ve Sutrave, K.. (2016). Mobile payment security, threats and challenges. Gainesville: 2016 Second International Conference on Mobile and Secure Services (MobiSecServ).

28. Zhang, P.. (2018). Why QR code payment develop well in China?. Research Topics In HCI Coursework, University of Birmingham.