KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

DOKTORA TEZİ

ONAY KODLU GÜVENLİ M-KUPON ALGORİTMASININ GELİŞTİRİLMESİ VE BİÇİMSEL ANALİZİ

KERİM YILDIRIM

KOCAELİ 2019

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ

ANABİLİM DALI

DOKTORA TEZİ

ONAY KODLU GÜVENLİ M-KUPON ALGORİTMASININ GELİŞTİRİLMESİ VE BİÇİMSEL ANALİZİ

KERİM YILDIRIM

Prof.Dr.Nevcihan DURU Danışman,	Kocaeli Üniv.	.....
Prof.Dr.Yaşar BECERİKLİ Jüri Üyesi,	Kocaeli Üniv.	.....
Doç.Dr.Gökhan DALKILIÇ Jüri Üyesi,	Dokuz Eylül Üniv.	.....
Doç.Dr.Ahmet SAYAR Jüri Üyesi,	Kocaeli Üniv.	.....
Doç.Dr.İbrahim ÖZÇELİK Jüri Üyesi,	Sakarya Üniv.	.....

Tezin Savunulduğu Tarih: 11.02.2019

ÖNSÖZ VE TEŞEKKÜR

Bu tez çalışması, müşterilerin indirim almak için kullandıkları m-kupon algoritmalarının güvenlik analizini yapmak ve müşteri ile satıcının haklarını koruyarak, tüm güvenlik kriterlerini karşılayan yeni bir m-kupon algoritması geliştirmek amacıyla gerçekleştirilmiştir.

Tez çalışmam süresince desteğini esirgemeyen, çalışmalarıma yön veren ve bana güvenen çok değerli hocam ve danışmanım Prof. Dr. Nevcihan DURU'ya sonsuz teşekkürlerimi sunarım.

Yüksek lisans öğrenimimden doktoraya başlama dönemine, oradan 02 Eylül 2013 tarihindeki vefatına kadar geçen dönemde, beni hep motive eden, bilgi ve tecrübeleriyle yönlendiren/yüreklendiren, danışmanlığımı yapan çok değerli hocam Yrd. Doç. Dr H.Engin DEMİRAY'ı rahmetle anar, minnetlerimi sunarım.

Tez danışma kurulu üyesi olarak görev yapan, bana bilgi ve tecrübeleriyle katkıda bulunan, değerli birikimlerini benimle paylaşan çok değerli hocam Prof. Dr. Yaşar BECERİKLİ'ye teşekkürlerimi sunarım.

Tez çalışmalarımın tüm aşamalarında bana bilgi, tecrübe ve yardımlarıyla katkıda bulunan, karşılaştığım her zorlukta desteğini ve zamanını esirgemeyen çok değerli hocam Doç. Dr. Gökhan DALKILIÇ'a teşekkürlerimi sunarım.

Hayatım boyunca bana güç veren en büyük destekçilerim, her aşamada sıkıntılarımı ve mutluluklarımı paylaşan sevgili eşim Özlem YILDIRIM'a, oğlum Ö.Deniz YILDIRIM'a, babam Ali YILDIRIM'a, annem Elif YILDIRIM'a teşekkürlerimi sunarım.

Şubat – 2019 Kerim YILDIRIM

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

$\|\|$	:	Birbirine bağlama sembolü
C_{ID}	:	M-kuponun kimlik bilgisi
E()	:	Şifreleme algoritması
$E(\ldots,KR_X)$	:	X'in gizli anahtarıyla yapılan şifreleme işlemi
$E(\ldots,KU_X)$	:	X'in açık anahtarıyla yapılan şifreleme işlemi
$E(\ldots,K_{XY})$	:	KXY simetrik anahtarı ile yapılan şifreleme işlemi
F	:	Üretici Firma
H()	:	Kriptografik özet fonksiyonu
ID_X	:	X'in kimlik bilgisi; X = M, F, R, P or U
KU_X	:	X'in açık anahtarı; X = M, F, R, P or U
KR_X	:	X'in gizli anahtarı; X = M, F, R, P or U
K_{XY}	:	X kullanıcısından Y kullanıcına gönderilen simetrik anahtar
K_{YX}	:	Y kullanıcısından X kullanıcına gönderilen simetrik anahtar
M_C	:	İndirim bilgisi
M_{kupon}	:	Müşteriye gönderilen m-kupon
MUC	:	Mobil cihazın eşsiz değeri
N_{XY}	:	X kullanıcısından Y kullanıcına gönderilen rasgele sayı
N_{YX}	:	Y kullanıcısından X kullanıcına gönderilen rasgele sayı
O	:	Onay kodu
PIN	:	Müşteri kodu
P	:	M-kupon sağlayıcı
R	:	Satıcı/kasiyer
S_f	:	Kasiyer tarafından üretilen rasgele sayı
S_m	:	Müşterinin mobil cihazı tarafından üretilen rasgele sayı
teklif	:	M-kupon bilgisi (tipi, oluşturulma zamanı, geçerlilik süresi vb.)
V_f	:	Kasiyer ve kupon sağlayıcılar arasında paylaşılan gizli anahtar
U, M, MM	:	Kullanıcı/müşteri
X	:	Kupon sağlayıcı ve kasiyerin sabit gizli anahtarı

Kısaltmalar

CSP	:	Communicating Sequential Processes (Sıralı İşlemlerle İletişim)
FDR	:	Failures Divergence Refinement (Hataları Uzaklaştırma Arıtma)
IEEE	:	The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IKEv1	:	Internet Key Exchange Phase 1 (İnternet Anahtar Değişimi Safha 1)
IKEv2	:	Internet Key Exchange Phase 2 (İnternet Anahtar Değişimi Safha 2)
ISO	:	International Organization of Standardization (Uluslararası Standartlar Teşkilatı)
IoT	:	Internet of Things (Nesnelerin İnterneti)
LBS	:	Location Based Services (Konum Tabanlı Servisler)
NFC	:	Near Field Communication (Yakın Alan İletişimi)
SMS	:	Short Message Service (Kısa Mesaj Hizmeti)

SPDL : Specification and Description Language (Tanımlama ve Açıklama Dili)
WOM : Word-Of Mouth (Ağızdan Ağıza, Kulaktan Kulağa)

ONAY KODLU GÜVENLİ M-KUPON ALGORİTMASININ GELİŞTİRİLMESİ VE BİÇİMSEL ANALİZİ

ÖZET

Günümüzde mobil cihazlar üzerlerinde barındırdıkları teknolojiler sayesinde günlük hayatın her alanına girmiş, günlük yaşantının bir parçası olmuşlardır. Bu uygulamalara örnek olarak yeni bir alan olan ve mobil cihazlarda kullanılan m-kupon uygulaması verilebilir. M-kupon, müşterilere özel indirimler vermek için kullanılan mobil bir kupondur. Mobil kupon kullanımının yaygınlaştırılabilmesi için gerekli olan önemli hususlardan birisi, kullanıcı güvenliğinin sağlanmasıdır. M-kuponun elde edilmesi ve kullanılması aşamasındaki güvenlik, sadece bilinen şifreleme algoritmaları kullanılarak sağlanamaz. Şifreleme algoritmaların olmazsa olmaz bir unsuru olmasına rağmen tek başına sadece şifreleme kullanılarak güvenlik garanti altına alınamaz. Bunlara ek olarak sürecin önemli bir parçası olan algoritmanın da güvenlik analizinin yapılması gerekmektedir. Bu kapsamda yapılan bu çalışmada, firmaların özel müşterilerine sağladığı özel indirimlerin müşterilerine ulaşabilmesi için kullanılan m-kupon algoritmalarının güvenlik analizini yapmak için, iki adet algoritma vaka analizi için seçildi. Hsueh ve Chen tarafından geliştirilen algoritmanın güvenlik analizi senaryolar üzerinden, Hsiang tarafından geliştirilen NFC tabanlı algoritmanın güvenlik analizi, oyun kuramı ve otomatik güvenlik algoritması doğrulama aracı Scyther kullanılarak yapıldı. Analiz çalışmasında saldırganın, iletişimi dinleyerek kuponların çoklu kullanımı, yeniden gönderme, müşterinin kimlik bilgilerinin çalınması, yetkisiz kupon kullanma/üretme, kuponun geçersiz hale getirilmesi, gizli anahtarın elde edilmesi saldırılarını yaparak, elde ettiği paketleri çözüp çözemediği, sistemi manipüle edip edemediği incelenmiştir. İnceleme sonucunda, Hsueh ve Chen tarafından geliştirilen algoritmanın, kuponun oluşturulması ve kuponun kullanılması aşamalarında, Hsiang tarafından geliştirilen algoritmanın, kuponun oluşturulması ve gizli anahtarın korunması aşamalarında güvenlik zafiyeti olduğu, bu açıklar kullanılarak saldırılar yapılabildiği tespit edilmiş ve tespit edilen açıklar için çözüm önerileri sunulmuştur. Elde edilen bilgi ve tecrübeler doğrultusunda tüm güvenlik kriterlerini sağlayan ve kullanıcıların haklarını ve verilerini koruyan yeni bir m-kupon algoritması tasarlanmıştır. Geliştirmiş olduğumuz algoritmanın saldırılara karşı ne kadar güçlü ve dayanıklı olduğunu görmek/göstermek için de Scyther aracı ile güvenlik analizi yapılmıştır.

Anahtar Kelimeler: Güvenlik Analizi, NFC, M-Kupon, Scyther, Veri Güvenliği.

DEVELOPMENT OF A SECURE M-COUPON SCHEME WITH CONFIRMATION CODE AND FORMALLY ANALIZATION OF THE SCHEME

ABSTRACT

Nowadays due to the technological development mobile devices equipped with new technologies have entered and become part of our lives. For instance, a novel issue used on mobile devices: m-coupon which is a special coupon and used to give special discount to the customers. One of the important things that mobile coupon usage needs to be widespread is ensuring of user security. M-coupon scheme can't be secured just using only known cryptographic algorithms. Although cryptographic algorithms are an essential part of the scheme, security cannot be guaranteed by using cryptographic algorithms alone. Additionally security analysis of the scheme which is the essential part of the process must be done thoroughly. In this context, to make security analysis of mobile coupon schemes which are used to deliver special discounts to the special customers, we have selected two schemes for case analysis. Security analysis of the scheme developed by Hsueh and Chen performed through scenarios; security analysis of the NFC-based scheme developed by Hsiang was performed using the game theory and formal security scheme validation tool Scyther. In the analysis, an attacker, by listening the established communication, established multiple cash-in attack, replay attack, impersonation attack, unauthorized coupon copying/generation, invalidation of the coupon attack and secret disclosure attack, then examined whether he can unpack the packages he obtained or can manipulate the system. The analysis showed that, Hsueh and Chen's scheme has weakness at the issuing and redemption phase, Hsiang's scheme has weakness at the issuing phase and securing the secret key, by using these vulnerabilities some attacks have been illustrated and solutions are proposed for these vulnerabilities. Then by using obtained knowledge and experience during these analysis, we have developed a new m-coupon scheme providing all security criteria to protect users' rights and data. To see/show how strong and durable the scheme, security analysis of the scheme is carried out with Scyther tool.

Keywords: Security Analysis, NFC, M-Coupon, Scyther, Data Security.

GİRİŞ

Mobil cihazlar günlük yaşantımızda arkadaşlarımızla konuşmanın yanı sıra sürekli temas halinde olma, moda, müzik dinleme, uzaktan ebeveynlik, televizyon programları ile etkileşim, video izleme, yeni insanlarla tanışma, mobil ticaret (Goggin, 2012), kullanıcının sağlık bilgilerini takip etme (Krishna ve diğ., 2009) gibi amaçlar için de kullanılmaktadır.

Ayrıca, mobil cihazlar üzerinde yaygın olarak kullanılmaya başlanılan sensörler/teknolojiler sayesinde yeni kullanım alanları ortaya çıkmaktadır. Fotoğraf çekmek için kullanılan flaşörün kalp atışını ölçmek için kullanılması (Gregoski ve diğ., 2012), mobil sensörler aracılığıyla kan basıncı, kan şekerinin ölçülmesi (Gregoski ve diğ., 2012), üç eksenli akselerometre sensörü kullanılarak kullanıcının yürüdüğünün, koştuğunun, oturduğunun, merdiven tırmandığının anlaşılması (Kwapisz ve diğ., 2011), özellikle yaşlı ve bakıma muhtaç insanların düştüğü zaman kullanabilecekleri düşme analizi uygulamaları (Yıldırım ve diğ., 2016) örnek olarak sayılabilir.

Bunlara ek olarak geleceği şekillendirebilecek bir teknoloji olan yakın alan iletişimi (near field communication - NFC) mobil cihazlarda yaygın olarak kullanılmaya başlanmıştır. NFC, ISO/IEC 18092:2013 (2013) standardında tanımlandığı şekilde 13,56 MHz frekansında çalışmaktadır. NFC teknolojisi kullanılarak mobil cihazlar için geliştirilen uygulamalara; cep telefonlarının banka kartı gibi kullanılması (Tan ve diğ., 2014; Ooi ve diğ., 2016), toplu taşımada bilet uygulaması (Schäfer ve diğ., 2017; Finžgar ve Trebar, 2011; D'silva ve diğ., 2017), turizm sektöründe bilet olarak kullanılması (Arslan ve diğ., 2016), eğlence/ulaşım alanında bilet yerine kullanılması (Ghìron ve diğ., 2009; Vives-Guasch ve diğ., 2012; Zang ve diğ., 2012) verilebilir.

Günümüzde NFC, nesnelerin internetinde (Internet of Things (IoT)) (Chaudhary ve Garg, 2014) en büyük teknolojilerden birisidir. Cisco tarafından yapılan teknik bir incelemeye göre (Evans, 2012) 2020 yılına kadar 50 milyar cihazın internete bağlanması beklenmektedir. Bu da IoT ve NFC teknolojilerinin ne kadar önemli

olduğunu göstermektedir. Bu nedenle önde gelen Telekom şirketleri yeni ürettikleri telefonlara NFC teknolojisini eklemektedir. iPhone bu özelliği iPhone 6 ve sonrası üretmiş olduğu modellere eklemektedir (Holton, 2014). Bu, cep telefonlarının alışverişte önemli bir rol oynayacağını göstermektedir. Cep telefonlarının başka bir sürü kullanım alanı bulunmaktadır. Bunlardan bazıları hemen hemen herkes tarafından kullanılırken bazıları hala emekleme aşamasındadır.

NFC özellikli cep telefonlarının kullanımı yaygınlaştıkça bu özellik kullanılarak geliştirilen algoritma/uygulamaların da sayısı artmaktadır. Bu uygulamalara örnek olarak hala gelişim sürecinde olan ve mobil cihazlarda kullanılmaya başlanan m-kupon uygulaması verilebilir.

Müşterilerin ilgisini çekmek için kullanılan birçok pazarlama yöntemi bulunmakta, müşteriler de ürünleri daha ucuza almak için araştırmalar yapmakta ve indirimleri takip etmektedir. İndirim kuponlarını kullanmak ürünleri daha ucuza almak için kullanılan yaygın yöntemlerden birisidir. Teknolojinin gelişmesiyle birlikte klasik kağıt kuponlar elektronik kupona (e-kupon) sonra da mobil kupona (m-kupon) dönüşmektedir. Mobil cihazların günlük hayatın içerisine bu kadar girdikleri göz önüne alındığında firmaların/satıcıların, müşterilerin ilgisini çekebilmek için m-kupon teknolojisini kullanmaları kaçınılmaz olacaktır. Sonuç olarak m-kupon teknolojisinin gelecek vadeden bir teknoloji olduğunu rahatlıkla söyleyebiliriz. M-kuponların kullanımıyla ilgili önemli sorunlardan birisi güvenliktir. Burada hem satıcının hem de müşterinin bilgilerinin güvenliğinden emin olunmalı, ayrıca sistem her iki taraf için de gereksiz gelir kaybına neden olmamalıdır.

M-kuponlar sayesinde firmalar, müşterilere ulaşmak için kart basma, basılan kartları dağıtma gibi maliyetlerden kurtulmakta, sadık müşteri programlarını özgürce uygulama, avantaj paketlerini (kupon) daha az maliyetle, istedikleri zaman, istedikleri müşteriye ulaştırma (target based marketing) (Hill ve diğ., 2006) şansını yakalamaktadırlar. M-kuponların temin edilme yöntemlerini dört kategori altında toplayabiliriz (Hsueh ve Chen, 2010):

Kategori I: Kısa mesaj servisi (SMS) ile,
Kategori II: Yetkilendirilmiş bir kupon sağlayıcının web sayfasından,
Kategori III: Konum tabanlı servislerle (Chincholle, 2002),

Kategori IV: Gazete, dergi, broşürlere eklenmiş radyo frekansı ile tanımlama (radio frequency identification - RFID) özellikli posterler aracılığı ile.

İndirim için kullanılan kuponlardan m-kuponun kullanımı için kağıt kuponlara ve e-kuponlara göre avantajları bulunmaktadır. Bunlar arasında; kullanımın daha kolay olması, telefonları sürekli müşterilerin yanında olduğu için unutulma ihtimalinin diğer kuponlara göre daha düşük olması, sadık müşteri kartlarının yerine kolaylıkla kullanılabilecek olması, firmaların özel müşterileri için özel indirimler yapabilmesine ve kuponları istediği zamanda dağıtabilmesine olanak sağlaması, müşterinin telefonunun alışveriş yaparken müşterinin bulunduğu konuma göre kullanabileceği kuponlarla ilgili bilgilendirme sağlayabilmesi, kuponların sadece istenilen müşteriler tarafından kullanılmasına olanak sağlaması sayılabilir.

Firmalar ve araştırmacılar m-kuponların kullanım oranlarını arttırmak için yeni yöntemler geliştirmeye ve daha güvenilir m-kupon algoritmaları/uygulamaları geliştirmeye çalışmaktadır. Bu kapsamda 2007 yılında Dominikus ve Aigner tarafından NFC tabanlı bir m-kupon algoritması (Dominikus ve Aigner, 2007) , 2008 yılında Hsiang ve Shih tarafından özet tabanlı (hash-based) NFC m-kupon algoritması (Hsiang ve Shih, 2009), 2009 yılında Hsiang ve Shih tarafından özet tabanlı NFC m-kupon algoritmasından esinlenerek geliştirilen QR (quadratic residue theorem) tabanlı NFC m-kupon algoritması (Hsiang ve Shih, 2009), 2010 yılında Hsueh ve Chen tarafından ağızdan ağıza/kulaktan kulağa yöntemi (word-of mouth - WOM) kullanılarak bir m-kupon paylaşım yöntemi önerilmiştir (Hsueh ve Chen, 2010). Önerilen algoritma (Hsueh ve Chen, 2010), m-kuponları doğrulamak için tek yönlü özet zinciri (hash chain) ve dijital imza kullanmaktadır. Park ve Lee tarafından 2013 yılında düşük maliyetli ve kısıtlı kaynaklarla kullanılabilen NFC tabanlı bir algoritma (Park ve Lee, 2013), 2014 yılında Hsiang tarafından NFC tabanlı m-kupon algoritması (Hsiang, 2014), yine Park ve Lee tarafından düşük hesaplama kapasitesine sahip NFC posterlerinde kullanılmak üzere bir algoritma (Park ve Lee, 2016) geliştirilmiştir. Chen ve arkadaşları tarafından 2016 yılında, güvenlik için açık anahtarlı şifreleme sistemi kullanılan, NFC tabanlı bir m-kupon algoritması geliştirilmiş (Chen ve diğ., 2016) ve 2016 yılında Yim tarafından, yine 2016 yılında Jiang ve arkadaşları tarafından yeni algoritmalar önerilmiş ve bu m-kupon algoritmalarının uygulamaları yapılmıştır (Yim, 2016; Jiang ve diğ., 2016). 2016

yılında Bartoli ve Medyet tarafından farklı bir yaklaşım sergilenmiş ve müşterinin herhangi bir kuponu herhangi bir ön düzenleme olmaksızın herhangi bir mağazada herhangi bir cihazını kullanarak alabilmesine ve kullanabilmesine olanak sağlayan bir yapı önerilmiştir (Bartoli, 2016).

Hsiang, geliştirmiş olduğu algoritmayı (Hsiang, 2014), Feldhofer tarafından geliştirilen algoritmayı (Feldhofer ve diğ., 2004) ve Aigner tarafından geliştirilen algoritmayı (Aigner ve diğ., 2007) referans alarak tasarlamış ve bu iki algoritmayla karşılaştırmıştır. Feldhofer tarafından geliştirilen algoritma (Feldhofer ve diğ., 2004) açık anahtarlı şifreleme altyapıya sahiptir. Bu algoritmada müşteri m-kuponu pasif NFC etiketli bir posterden almakta ve sonrasında kasiyere vererek kuponu kullanmaktadır. Aigner ve arkadaşları tarafından geliştirilen algoritmada (Aigner ve diğ., 2007) NFC teknoloji kullanılarak geliştirilmiş ve simetrik şifreleme algoritmaları kullanılarak uygulanmıştır. Yeni bir m-kupon sistemi, uygulaması ile birlikte Yim tarafından sunulmuştur (Yim, 2016).

Yapılan bu çalışmaların bir kısmında sadece algoritma tanımlanırken (Hsueh ve Chen, 2010; Dominikus ve Aigner, 2007; Hsiang ve diğ., 2009; Hsiang ve Shih, 2009; Park ve Lee, 2013; Hsiang, 2014), diğer bir kısmı ise algoritmanın uygulamasını da içermektedir (Chen ve diğ., 2016; Yim, 2016; Jiang ve diğ., 2016). Burada bahsedilen m-kupon algoritmalarının yanı sıra m-kuponların kullanımına yönelik araştırmalar da bulunmaktadır (Danaher ve diğ., 2015).

Yapılan tüm bu uygulamaların, geliştirilen tüm sistemlerin amacı kullanıcıların hayatlarını kolaylaştırmaktır. Ancak uygulama geliştiricilerin kullanıcılara ait özel bilgilerin güvenliğini sağlama, kimlik, sağlık, finans, alış veriş, vb. bilgilerin yetkisiz kişilerin eline geçmesini engelleme hususlarına dikkat etmesi gerekmektedir.

İşte tam bu noktada geliştirilen uygulamalara ait algoritmaların, protokollerin ve geliştirme araçlarının güvenliği, güvenlik analizi devreye girmektedir. Ayrıca, yapılan işlemlerde araya girebilecek bir saldırgana karşı veri transfer protokolünün de güvenli olması gerekmektedir. Nitekim 2015 yılında, Amerika'nın en büyük ikinci sağlık sigortası şirketi Anthem'in sistemlerindeki güvenlik açıklarından faydalanılarak, 80 milyon vatandaşın kişisel verileri çalınmıştır (Mathew ve Yadron,

2015). Bu da alınması gereken güvenlik önlemlerinin ne kadar ciddi olduğunu gösteren bir örnektir.

Motivasyon: Kullanıcılar için geliştirilen çok sayıda uygulama bulunmasına ve her geçen gün sayılarının artmasına rağmen uygulamalara ait güvenlik analizleri bu artışa paralel olarak ilerlememektedir. Yapılan çalışmalarda güvenlik analizinden ya hiç bahsedilmemekte ya da sadece yüzeysel olarak anlatılmaktadır. Bu alanda yeterli çalışmanın olmaması ve güvenli olduğu iddia edilen algoritmaların bile güvenlik analizlerinin hangi yöntemle yapıldığına yönelik bir açıklamanın çoğunlukla bulunmaması gerçeği, bu tezin esin kaynağı olmuştur. Konu olarak da, yakın gelecekte yaygın bir kullanım alanı bulacağı değerlendirilen m-kuponların güvenlik analizi seçilmiş ve güvenli bir m-kupon algoritmasının geliştirilmesi hedeflenmiştir.

Bu kapsamda m-kupon algoritmaları içerisinden iki adet algoritma (Hsueh ve Chen tarafından geliştirilen m-kupon algoritması (Hsueh ve Chen, 2010) ile Hsiang tarafından geliştirilen m-kupon algoritması (Hsiang, 2014) vaka analizi yapılmak üzere seçilerek güvenlik analizleri yapılmıştır. Hsueh ve Chen tarafından geliştirilen m-kupon algoritmasının güvenlik analizi senaryolar üzerinden, Hsiang tarafından geliştirilen m-kupon algoritmasının güvenlik analizi ise JavaScript kullanılarak geliştirilen web tabanlı simülasyon üzerinden oyun kuramı yöntemi ile yapılmıştır. Ayrıca Hsiang tarafından geliştirilen m-kupon algoritması, güvenlik protokollerinin/algoritmalarının doğrulanması için kullanılan Scyther aracı kullanılarak da analiz edilmiş, ardından önerilen çözümlerin başarılı olup olmadığı yine Scyther ile kontrol edilmiştir.

Daha sonra, yapılan bu analiz çalışmaları sonucunda elde edilen bilgiler doğrultusunda, tüm güvenlik kriterlerini sağlayan yeni bir m-kupon algoritması; onay kodlu güvenli m-kupon algoritması (M-Coupon protocol With Confirmation Code (MCWCC)) geliştirilmiş ve ne kadar güvenli olduğunu ispatlamak için algoritmanın analizi için güvenlik algoritmalarının doğrulanması amacıyla kullanılan Scyther analiz aracı kullanılmıştır. Ayrıca JavaScript kullanarak MCWCC'in web tabanlı bir simülasyonunu yapılmıştır. Bildiğimiz kadarıyla bu algoritma, güvenlik analizi algoritmanın geliştiricileri tarafından güvenlik protokollerinin/algoritmalarının doğrulanması amacıyla kullanılan araçlar ile yapılan ilk m-kupon algoritmasıdır.

Çalışma düzeni şu şekildedir: birinci bölümde güvenlik analizi ile ilgili bilgiler verilmiş, ikinci bölümde Hsueh ve Chen tarafından geliştirilen m-kupon algoritmasının güvenlik analizi, üçüncü bölümde Hsiang tarafından geliştirilen m-kupon algoritmasının güvenlik analizi yapılmış, dördüncü bölümde yeni geliştirilen m-kupon algoritması (MCWCC) detaylı olarak açıklanmış ve güvenlik analizi yapılmıştır.

1. MATERYAL VE METOT

Yeni bir ürün alırken istenilen ürünün en uygun fiyata alınmasıdır. Bu nedenle de potansiyel alıcılar alışveriş yapmadan önce inceleme/araştırma yaparlar. Günümüzde araştırma yapmadan alışveriş yapan neredeyse yoktur. Özellikle internetin olanaklarını düşünüldüğünde istenilen ürünün fiyatları küçük bir araştırmayla (örnek: fiyat karşılaştırması yapan siteler aracılığıyla) elde edilebilmektedir.

Satıcılar sürekli müşterilerin nabzını tutmakta, ürünlerini pazarlamak için yeni yöntemler geliştirmektedir. Ayrıca müşterileri kendilerine bağlamak ve sürekli alışveriş yapmalarını garanti altına almak için müşteri sadakat kartları çıkartmakta, bu kart sahiplerine özel indirimler sunmaktadırlar. Teknolojinin gelişmesiyle birlikte artık bu basılı kartların yerini mobil cihazlar almaya başlamıştır. Mobil cihazlar sürekli yanımızda olduğu için firmalar tekliflerini e-posta veya SMS aracılığıyla anında gönderebilmektedir.

Mobil cihazların üzerine eklenen NFC özelliği sayesinde kullanıcıları tanımlamak için kullanılacak ID değeri “secure element” içerisinde saklanabilmekte, böylelikle kullanıcıların kimlikleri kontrol edilebilmektedir.

Teknoloji her alana girmiş olmasına rağmen kullanımı konusunda sürekli endişeler bulunmaktadır. Bu endişeleri ortadan kaldırmanın en etkili ve kolay yolu geliştirilen uygulamaların güvenlik analizlerinin yapılması, dolayısıyla uygulamanın güvenilir olduğunu kullanıcılara ispatlanmasıdır.

Firmalar her gün yeni ürünler piyasaya sürmekte ve tüketicilerin ilgisini çekmek için değişik yöntemler kullanılmaktadır. Reklam bunların en başında gelen yöntem olmasına rağmen kalıcı olmanın yolu güvenilir olmaktan geçmektedir. Kimse bir ürün alırken veya kullanırken para kaybetmek istemez. Bütçelerine göre en iyi ürünü en uygun fiyata almak isterler. Bunlara örnek olarak arabaların çarpma testleri, sürücünün, yolcuların ve yayaların korunması konusunda yapılan testler verilebilir.

Peki, sürekli harcama yaptığımız, kullandığımız veya yeni geliştirilen teknolojilerle birlikte hayatımıza giren ürünler?

Durum onlar için de geçerlidir. Araçların testleri kısmen de olsa gözle de görülebilir. Ancak bazı ürünler vardır ki bunlar ancak özel yöntemlerle analiz edilebilir. Örnek olarak iletişimin (veri transferinin) güvenlik analizi nasıl yapılır?

Geliştirilen sistemlerin güvenliklerini sağlamak için şifreleme kullanılması algoritma güvenliğinin hayati bir parçası olmakla birlikte, güvenliğin sağlanması için tek başlarına yeterli değildirler. Bunlara ek olarak algoritmanın bir bütün olarak da ele alınması ve güvenlik analizinin yapılması gereklidir. Yapılacak olan güvenlik analizi gizlilik, kimlik kontrolü, bütünlük, doğrulanabilirlik ve değiştirilememe basamaklarını içermelidir.

Güvenlik analizlerinin doğru yapılması sadece müşteriler için değil satıcılar için de çok önemlidir. Çünkü müşteri ürünler daha ucuza satın almak isterken satıcı da gereksiz kayıplar yaşamak istemez. Dolayısıyla algoritma hem müşteri hem de satıcının haklarını koruyabilmelidir.

Bunlara ek olarak NFC Teknik Kılavuzunda (GSM Association, 2007) m-kupon algoritmalarının, ortadaki adam, kimliğine bürünme, yeniden gönderme, gizlice dinleme, yetkisiz kupon çoğaltma/üretme, çoklu kupon kullanma gibi saldırılara karşı dayanıklı olması gerektiği belirtilmektedir. Bazı ataklar, şifreli metne hiç dokunmadan sadece araya girerek elde edilecek verilerle yapılabilmektedir: Ortadaki adam ve yeniden gönderme saldırıları gibi.

M-kupon kullanımının yaygınlaştırılabilmesi için de gerekli olan önemli hususlardan birisi, kullanıcıların (müşteri, satıcı) güvenliğinin sağlanmasıdır. Bu kapsamda, yeni geliştirilecek m-kupon uygulamalarının güvenlik analizlerinin tasarım aşamasında yapılarak kullanıma sunulmasının, hem müşteriler hem de firmalar açısından hayati derecede önemli olduğu ortaya çıkmaktadır. Örneğin 2016 yılında Yim tarafından geliştirilen kupon sisteminin (Yim, 2016) güvenlik analizinin nasıl yapıldığı sunulan çalışmada belirtilmemiş, 2017 yılında Jiang ve arkadaşları tarafından geliştirilen m-kupon dağıtımı modelinin (Jiang ve diğ., 2016) saldırılara karşı güvenlik analizinin gelecek çalışmalar kapsamında yapılacağı belirtilmiş, 2016 yılında Bartoli ve Medyet

tarafından geliştirilen algoritmada (Bartoli ve Medvet, 2016) güvenliğin açık anahtarlı şifreleme sistemi üzerine kurulduğu belirtilse de bunun haricinde güvenlik ve güvenlik analizi ile ilgili detaylı bir açıklama yapılmamıştır. Özellikle NFC teknolojisinin günlük yaşamın her alanına girmeye başladığı düşünüldüğünde bu hususa daha fazla dikkat edilmesi gerektiği ortaya çıkmaktadır.

Algoritmaların güvenlik analizlerini yapmak için yöntem olarak senaryolar, oyun kuramı, simülasyonlar veya güvenlik protokolleri/algoritmaları analiz araçları (CASPER/FDR, AVISPA, SCYTHER analiz araçları gibi) kullanılmaktadır. Örneğin Alshehri ve arkadaşları tarafından, Dominikus ve Aigner'in birlikte geliştirdikleri algoritmanın (Dominikus ve Aigner, 2007) güvenlik analizi CASPER/FDR kullanılarak yapılmış, analiz sonucunda (Alshehri ve diğ., 2013), m-kuponu kullanacak müşterinin imzayı üretirken kasiyerin kimlik bilgilerini kullanmadığı tespit edilmiş, bu güvenlik açığı sayesinde de saldırganın yetkisiz olmasına rağmen kupon kullanabildiği gösterilmiştir. Ayrıca, Alshehri tarafından tez çalışması olarak (Alshehri, 2015) Hsiang ve arkadaşları tarafından geliştirilen özet tabanlı NFC m-kupon algoritmasının (Hsiang ve Shih, 2009) ve QR tabanlı NFC m-kupon algoritmasının (Hsiang ve diğ., 2009) güvenlik analizi CASPER/FDR kullanılarak yapılmıştır. Yapılan analiz sonucunda özet tabanlı algoritmanın gizlilik ve sahtecilik (Confidentiality and Forgery Protection) saldırılarına karşı güvenli olduğu ancak veri bütünlüğü ve çoklu kupon kullanımı (Data Integrity and No Multiple Cash-in) saldırılarının yapılabildiği tespit edilmiştir. QR tabanlı NFC algoritması üzerinde yapılan analiz çalışmasında ise algoritmanın özet tabanlı algoritmaya göre daha iyi olduğu ancak algoritmada, kullanıcının kimlik doğrulama bilgilerinin doğru bir şekilde m-kuponuyla ilişkilendirilmediği bu nedenle de algoritmaya kimlik doğrulama (User Authentication) saldırısının yapılabildiği belirtilmiştir (Alshehri, 2015).

Geliştirilen bu m-kupon algoritmalarının, müşterilerin ve firmaların haklarını korudukları, güvenli oldukları ve saldırılara karşı dayanıklı oldukları iddia edilse bile, bu iddiaları destekleyecek ve algoritmaların istenilen güvenlik kriterlerini karşıladığını ispatlayacak bir kanıt sunulmadığı için, yapılan testlerin yüzde yüz güvenilir olduğunu söylemek mümkün değildir.

NFC tabanlı olarak geliştirilen mobil uygulamalara/algoritmalara yönelik olarak güvenlik konusunda yapılan çalışmalara örnek olarak yatan hastalara verilen ilaçların NFC teknolojisi ile güvenli bir şekilde takip edilmesi (Özcanhan ve diğ., 2014) verilebilir. NFC'nin güvenliği ile ilgili 2006 yılında Haselsteiner ve Breitfuß tarafından (Haselsteiner ve Breitfuß, 2006), 2007 yılında Dominikus ve arkadaşları tarafından (Dominikus ve Aigner, 2007) olası saldırılar hakkında çalışmalar yayınlamıştır. Ancak, her ne kadar m-kuponların uygulanabilirliği ve performans analizine yönelik çalışmalar (Hinarejos ve diğ., 2019) olsa da, güvenlik analizi yapılan bu çalışmalar ve m-kupon algoritmaları incelendiğinde, m-kupon algoritmalarının güvenlik analizine yönelik olarak sadece Alshehri ve arkadaşları tarafından yapılan çalışmaların (Alshehri ve diğ., 2013; Alshehri, 2015) olduğu tespit edilmiştir.

Geliştirilen uygulamaların güvenlik analizlerinin tasarımcıları tarafından geliştirme aşamasında yapılması gerektiği halde gerçek durum bu şekilde değildir. Geliştirilen uygulamaların güvenlik analizlerinin nasıl yapıldığından, hangi yöntem ve araçların kullanıldığından genellikle bahsedilmemektedir. Durum böyle olunca da kullanıcılar uygulamalara temkinli yaklaşmakta, güvenilir olduğunu düşünmediği uygulamaları kullanmamaktadır.

Uygulamalar kullanıcıların verilerini koruyabiliyor mu, kullanışlı mı, işlerine yarar mı, kullanımı kolay mı soruları sorulduktan sonra tercih edilmektedir. Veri gizliliği ve güvenliği hem kullanıcıların hem de ürünü hizmete sunanların birinci önceliğidir. Dolayısıyla mutlaka güvenlik analizleri yapılmalı ve nasıl yapıldığı şeffaf bir şekilde paylaşılmalıdır.

Bu kapsamda NFC tabanlı uygulamaların yakın bir gelecekte yaygın olarak kullanılacağı değerlendirilmiş ve m-kupon algoritmalarının güvenlik analizinin yapılmasına karar verilmiştir. Yapılan bu çalışmada vaka analizi olarak, m-kupon algoritmaları içerisinden güncel olan algoritmalardan olan ve yaptığımız araştırmalarda bu algoritmaların güvenlik açıklarına değinen bir çalışmanın olmaması nedenleriyle Hsueh ve Chen tarafından geliştirilen m-kupon algoritması (Hsueh ve Chen, 2010) ve Hsiang tarafından geliştirilen NFC tabanlı m-kupon algoritması (Hsiang, 2014) seçilmiş ve güvenlik analizleri yapılmıştır.

Hsueh ve Chen tarafından geliştirilen m-kupon algoritması çok bilinen algoritmalardan birisi olmakla birlikte yapısının genel m-kupon yapısı ile aynı olması tercih nedeni olmuştur. Bu algoritmanın güvenlik analizi hazırlanan senaryolar üzerinden yapılmıştır. Senaryolarda algoritmanın doğal üyeleri olan üretici firma (F), kupon sağlayıcı (P), satıcı/kasiyer (R) ve kullanıcı/müşteri (MM) ile birlikte saldırgan yer almıştır. Saldırgan kimi zaman sadece iletişimi gizlice dinleyerek kimi zaman da ortadaki adam saldırısı ile iletişime müdahale ederek saldırı gerçekleştirmiştir. Senaryolarda, kullanıcıların gelir kaybına uğramaması için alınan önlemler incelenmiş, gizlice dinleme, ortadaki adam saldırısı ve kasiyerin kendisinin saldırgan olması durumları değerlendirilerek algoritma analiz edilmiştir. Yapılan analiz çalışması ikinci bölümde anlatılmıştır.

Hsiang'ın tek başına ve/veya arkadaşları ile birlikte geliştirdiği m-kupon algoritmaları (Hsiang ve Shih, 2009; Hsiang ve diğ., 2009; Hsiang, 2014) arasında yer alan bu algoritma (Hsiang, 2014) 2014 yılında Hsiang tarafından tek başına yapılmış bir çalışmadır. Bu algoritma güncel olmasının yanı sıra kullanımının ve uygulanabilirliğinin kolay olması, uygulanabilmesi için yapıda sadece firmanın ve müşterinin yeterli olması (ilave bir kupon sağlayıcıya ihtiyaç duyulmaması ve firmanın kendi kuponlarını dağıtabilmesi), firmaların kendi dinamikleri ile sistemi idame edebilmelerine olanak tanıması nedenleriyle seçilmiştir. Hsiang tarafından geliştirilen m-kupon algoritmasının (Hsiang, 2014) güvenlik analizi için Oyun Kuramının Sıfır Toplamı Modeli (kazan ya da kaybet) (Myerson, 2013) kullanılmış ve bu amaçla simülasyon geliştirilmiştir. Simülasyon web (HTML) tabanlı olarak JavaScript kullanılarak tasarlanmış, algoritmanın doğal üyeleri olan müşteri, kupon sağlayıcı ve kasiyere ek olarak saldırgan simülasyona dâhil edilmiş ve bu oyuncular m-kuponun elde edilmesi ve kullanılması aşamalarında yer almıştır. Saldırganın tüm trafiği dinleyerek elde ettiği paketlerden algoritmanın doğal üyelerine (müşteri, kupon sağlayıcı ve kasiyer) ait gizli verileri elde edip edemediği incelenmiş, bu verileri kullanarak sistemi kandırabiliyorsa oyunu saldırganın kazandığı, aksi durumlarda ise saldırganın kaybettiği ve algoritmanın güvenli olduğu sonucuna ulaşılmıştır.

Ayrıca Hsiang tarafından geliştirilen algoritmanın analizi için, oyun kuramı ve simülasyonla analiz yöntemlerine ilave olarak, algoritmaların güvenlik analizi için

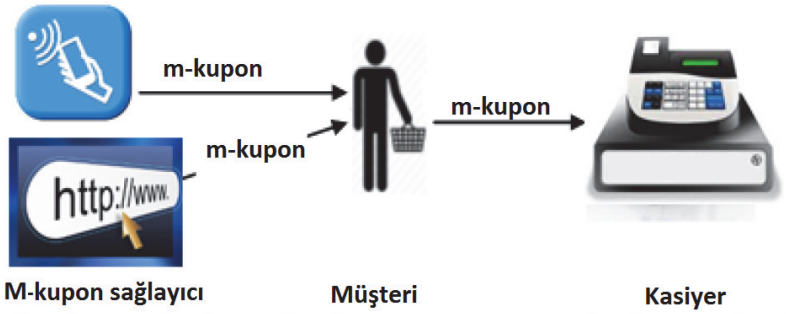
protokol/algoritma güvenlik analiz araçlarından Scyther (Cremers, 2008) kullanılarak hem algoritmanın güvenlik analizi yapılmış, hem Oyun Kuramı ve simülasyon ile yapılan tespitlerin doğruluğu kontrol edilmiş hem de sunulan çözüm önerilerinin güvenilir olup olmadığı analiz edilmiştir. Saldırıların nasıl yapıldığı üçüncü bölümde anlatılmıştır.

Daha sonra, bu analiz çalışmaları sonucunda elde edilen bilgiler doğrultusunda yeni ve güvenli bir m-kupon algoritması geliştirilmiş, geliştirilen onay kodlu m-kupon algoritması (MCWCC) detaylı olarak dördüncü bölümde anlatılmıştır. Sunulan bu algoritmanın çok bilinen saldırılara karşı (kimliğine bürünme, ortadaki adam, gizlice dinleme, yeniden gönderme, veri değiştirme, yetkisiz kupon çoğaltma/üretme, çoklu kupon kullanımı saldırıları) güvenlik analizi yapılmıştır. Ayrıca hem müşterinin hem de firma/satıcının verilerinin en yüksek seviyede korunup korunamadığını analiz etmek için, güvenlik protokollerinin/algoritmalarının doğrulanması amacıyla kullanılan Scyther analiz aracı ile algoritma analiz edilmiştir. Scyther ile yapılan analiz sonucunda algoritmanın tüm güvenlik kriterlerini karşıladığı ispat edilmiştir. Algoritmanın Scyter aracı için yazılan kodları Ek-Ç'de, JavaScript kullanarak yapılan MCWCC'in web tabanlı bir simülasyonunun sözde kodları Ek-D'de verilmiştir.

2. HSUEH VE CHEN M-KUPON ALGORİTMASI

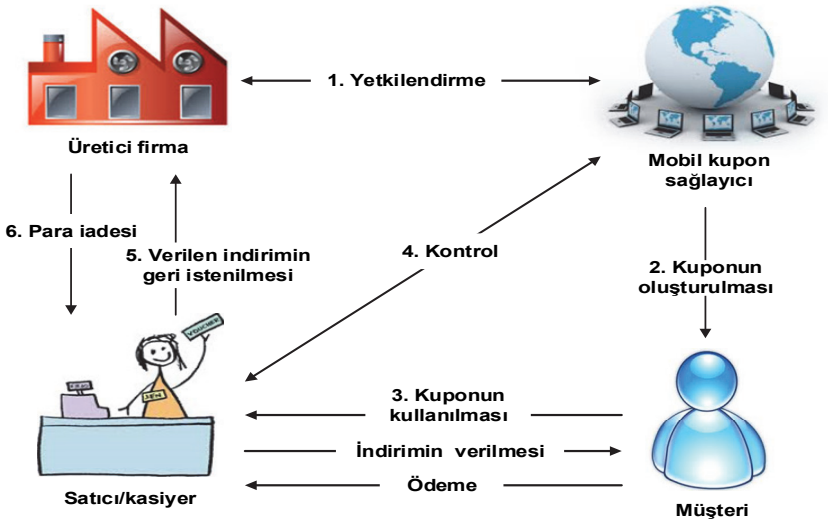
2.1. Algoritmanın Genel Yapısı

Hsueh ve Chen tarafından geliştirilen algoritma (Hsueh ve Chen, 2010) temel olarak Şekil 2.1'de gösterilen genel m-kupon kullanımı ile aynı yapıdadır. Bu yapıda algoritmada dört unsur yer almaktadır: Üretici Firma (F), Mobil Kupon Sağlayıcı (P), Satıcı/Kasiyer (R) ve Müşteri (MM). Bahse konu algoritmanın genel yapısı Şekil 2.2'de gösterilmiştir.



Şekil 2.1. Genel m-kupon kullanımı

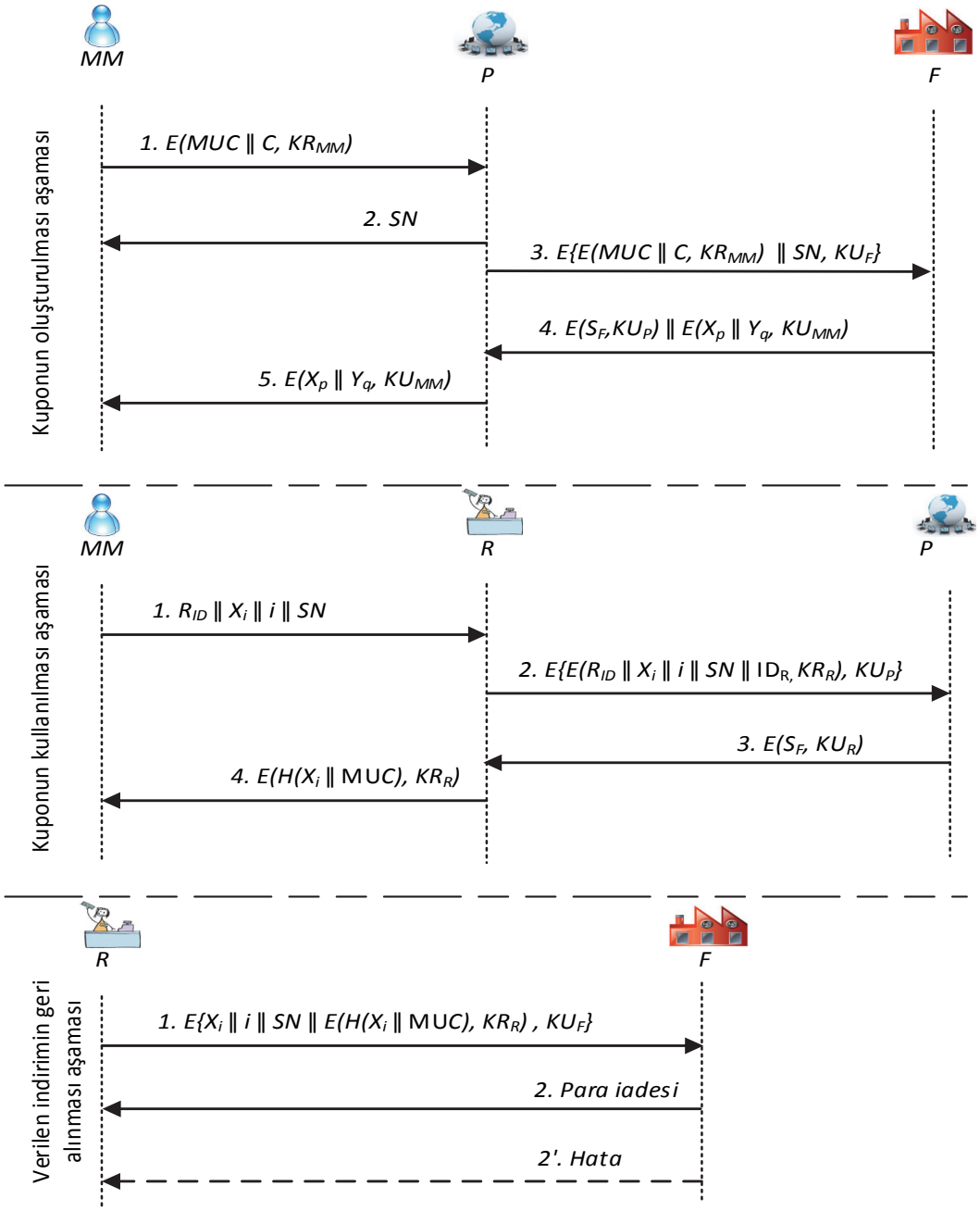
Birinci adımda üretici firma F kuponları müşterilere dağıtmak için bir kupon sağlayıcıyı P yetkilendirir. Müşteriler MM kuponları m-kupon sağlayıcı üzerinden temin etmektedir. Bu aşama kuponların oluşturulması aşamasıdır (issuing phase). Kuponun kullanılması aşamasında ise müşteri istemiş olduğu indirimi alabilmek için kasiyere verir. Kasiyer de müşterinin istemiş olduğu indirimin hala geçerli olup olmadığını kontrol etmek için kuponu kupon sağlayıcıya gönderir. Eğer kuponun hala geçerli olduğu onaylanırsa kasiyer müşterinin istemiş olduğu ürünü indirimli olarak verir. Müşterinin istemiş olduğu indirimi veren kasiyer (satıcı) gelirinin bir kısmını kaybetmiştir. Kasiyer kaybettiği bu geliri üreticiden geri alabilmek ve kuponun tekrar kullanımını engellemek için kullanım bilgilerini üreticiye gönderir.



Şekil 2.2. Genel m-kupon algoritma yapısı (Hsueh ve Chen, 2010)

Hsueh ve Chen algoritması güvenlik için açık anahtarlı şifreleme sistemini kullanmaktadır. Ayrıca veri bütünlüğünü/tutarlılığını sağlamak için özet fonksiyonu (hash function) ve dijital imza da kullanılmaktadır. Bu algoritmada müşteriler iki kategoriye ayrılmaktadır: hedeflenen müşteri kitlesi (targeted members) (MM) ve normal müşteriler (non- targeted members). Hedeflenen müşterilerin algoritma içindeki yeri Şekil 2.2'de görülebilir. Algoritmada MM aktif olarak iki aşamada yer almaktadır: kuponun oluşturulması aşaması ve kuponun kullanılması aşaması.

Burada yapmış olduğumuz çalışmada algoritmanın sadece hedeflenen müşteriler için kısmı incelenmiş ve analiz edilmiştir. Çünkü en büyük indirimler bu müşteri kitlesine uygulanmaktadır. Algoritmanın yapısı Şekil 2.3'te, kullanılan sembollerin açıklamaları simgeler ve kısaltmalar dizini altında verilmiştir.



Şekil 2.3. Hsueh ve Chen'in m-kupon algoritması (Hsueh ve Chen, 2010)

2.1.1. Kuponun oluşturulması aşaması

Kuponun oluşturulması aşaması beş adımdan oluşmaktadır. İlk adımda MM kendi gizli anahtarını kullanarak MUC ve C değerlerini şifreler ve dijital imza elde eder, daha sonar m-kuponu elde etmek için üretmiş olduğu dijital imzayı P'ye gönderir. İkinci adımda P SN değerini üreterek MM'e gönderir. Üçüncü adımda özet zincirini (hash chain) ve S_F değerlerini F'den almak için P, SN değerini ve MM'den gelen değerleri F'nin açık anahtarıyla şifreler ve F'ye gönderir. Daha sonra dördüncü

adımda F X_p, Y_q ve S_F değerlerini üreterek P'ye gönderir. Burada S_F P'nin açık anahtarı ile, X_p ve Y_q ise MM'in açık anahtarı ile şifrelenmektedir. P, S_F değerini aldıktan sonra kendi gizli anahtarı ile şifreyi çözer ve Eşitlik (2.1) ile gösterilen değerleri MM'e gönderir. MM gelen değerleri kendi gizli anahtarı ile çözer. Böylelikle kuponun oluşturulması aşaması tamamlanmış olur.

$$E(X_p \,||\, Y_{q,} KU_{MM}) \tag{2.1}$$

2.1.2. Kuponun kullanılması aşaması

Bu aşamada, MM istemiş olduğu indirimi alabilmek için, m-kuponu satıcıya/kasiyere sunmak zorundadır. R kendisine sunulan m-kuponun geçerliliğini kontrol etmek için m-kuponu P'ye gönderir. P tarafından yapılan kontroller sonucunda kuponun geçerli olduğunu tespit edilirse onay bilgisi önce R'ye, oradan da MM'e gönderilir.

İlk adımda müşteri X_0, X_i, ID_R ve MUC değerlerini kullanarak R_{ID} değerini hesaplar Eşitlik (2.2).

$$R_{ID} = H\,(X_0 \,||\, X_i \,||\, ID_R \,||\, MUC) \tag{2.2}$$

Daha sonra i'nci m-kuponu kullanmak için R_{ID}, X_i, i ve SN değerlerini R'ye gönderir.

İkinci adımda R müşteriden gelen verilere kendi ID değerini (ID_R) ekleyerek tamamını gizli anahtarı ile şifreler. R bu değerleri P'nin açık anahtarı ile şifreleyerek P'ye gönderir. Burada R'nin gizli anahtarı ile yapılan işlem ile göndericinin kimliği, P'nin açık anahtarı ile yapılan işlem ile de verinin gizliliği garanti altına alınmış oldu.

Üçüncü adımda P, R'den gelen verileri kontrol eder ve SN değerini kullanarak S_F değerini elde eder. Daha sonra S_F değerini sadece R tarafından açılmasını garanti altına almak için R'nin açık anahtarı KU_R ile şifreler ve R'ye gönderir.

Dördüncü adımda eğer gönderilen verilerin kontrolü esnasında bir problem ortaya çıkmazsa R Eşitlik (2.3)'ü hesaplayarak onay cevabı olarak MM'e gönderir. MM gelen veriyi kontrol etmek için kendisinde bulunan değerlerle Eşitlik (2.4)'ü hesaplar ve elde ettiği sonucu Eşitlik (2.3) ile kendisine gönderilen değerle karşılaştırır.

$$E(H(X_i \,||\, MUC), KR_R) \quad (2.3)$$

$$H(X_i \,||\, MUC) \quad (2.4)$$

2.1.3. Verilen indirimin geri alınması aşaması

R müşterinin istemiş olduğu indirimi vererek ürünü normalin daha altında bir fiyata satmış ve gelirinin bir kısmını kaybetmiş oldu. R kaybetmiş olduğu bu geliri geri alabilmek için F'ye kullanılan m-kupon bilgilerini gönderir. F gelen verileri kontrol ettikten sonra sorun çıkmazsa verilen indirimi R'ye geri verir. Aksi durumlarda hata mesajı gönderir.

2.2. Algoritmanın Güvenlik Analizi

2.2.1. Kuponun oluşturulması aşamasının güvenlik analizi

Kuponun oluşturulması aşamasında MM, MUC ve C değerlerini gizli anahtarı ile imzalayarak P'ye göndermektedir. Güvenlik açığı da burada ortaya çıkmaktadır. Eğer bir saldırgan Şekil 2.4'te gösterildiği gibi MM ve P arasındaki iletişimi dinlerse MUC ve C değerlerini elde eder. Şöyle ki, saldırgan iletişimi dinleyerek Eşitlik (2.5) ile gösterilen veriyi elde eder, MM'in açık anahtarını kullanarak şifreyi çözer ve MUC ve C değerlerini elde etmiş olur.

$$H(MUC \,||\, C, KR_{MM}) \quad (2.5)$$

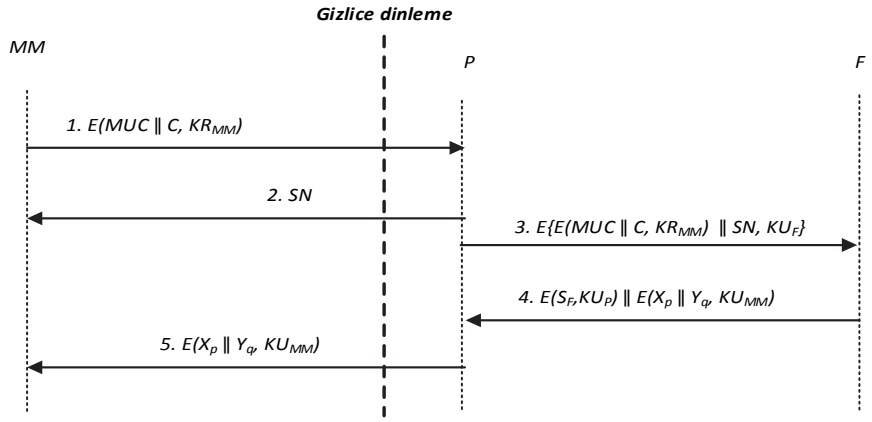
MUC değerinin elde edilmesi demek herhangi birisinin MM'i taklit edebilmesi yani o imiş gibi davranabilmesi anlamına gelmektedir. Çünkü MM'in kimliğinin kontrol edilmesi için kullanılan tek değer olan MUC, saldırganın eline geçmiştir. Örneğin saldırgan MUC değerini kullanarak kupon sağlayıcıya başka bir kupon için talep gönderebilir, almış olduğu kuponu asıl müşteri olan MM'in yerine kullanabilir ve bundan MM'in haberi bile olmaz. Algoritmada MM'in güvenlik kontrolü sadece MUC değeri üzerinden yapıldığı için burada P kiminle iletişim kurduğunu anlayamaz ve talep edilen m-kuponu MUC değerini kim gönderdiyse ona gönderir.

2.2.1.1. Atak senaryoları

M-kuponlar birçok şekilde elde edilebilmektedir. Bu metotlar dört kategori altında (Hsueh ve Chen, 2010) sınıflandırılmış olup kategorilerin detayları giriş kısmında anlatılmıştır.

Senaryo I: Eğer P ile MM arasında kurulan iletişimde (Şekil 2.4'te 2'nci adımdan 5'nci adıma kadar olan işlemler) mesajlar SMS aracılığı ile gönderilirse bu atak kategori I için uygulanamayabilir. Kategori I'e bu atağı uygulayabilmek için saldırıya bir adım daha eklenmesi gerekmektedir. Saldırganın MM'in yerine geçebilmesi için F'in sunucularında saklanan ve MM'e ait olan telefon numarasının istenilen başka bir numara ile (örneğin saldırganın kendi numarası) güncellenmesi gerekmektedir. Bu noktada da F'in sunucularında saklanan MM'e ait bilgilerin güvenliğinin nasıl sağlandığı hususu devreye girmektedir. Eğer güvenlik mekanizması yeterince güçlü değilse saldırgan bu profili güncelleyerek atağı gerçekleştirebilir. Eğer süreç SMS üzerinden işlemeseydi saldırgan, asıl müşterinin profilini değiştiremese bile, müşteriye ait olan MUC değerini elde edebilecek ve MUC değerini kullanarak saldırıyı rahatlıkla yapabilecekti.

Senaryo II: Bu atak m-kuponların web sayfasından indirildiği kategori II'ye uygulanabilir. Çünkü saldırgan müşteri ile kupon sağlayıcı arasındaki iletişime müdahale edebilir.



Şekil 2.4. Kuponun oluşturulması aşamasında iletişimi dinleme

Senaryo III: Kategori III için uygulanacak saldırı, LBS'in yapısı müşterinin konumuna göre yapılan mobil ticareti kapsaması nedeniyle, kategori I için

uygulanacak olan saldırıya benzemektedir. Bu kategoride kuponlar hedef kitlede yer alan müşteriye SMS ile gönderilmekte/teklif edilmektedir.

Senaryo IV: Kategori IV'te, NFC teknolojisinin yapısı nedeniyle saldırgan müşteri ile NFC tabanlı poster (m-kuponu müşteriye vermek için kullanılan bir poster) arasındaki iletişime müdahale edemez. Ancak bu durumda da saldırı farklı şekilde gerçekleştirilebilir: Saldırgan sahte bir NFC poster hazırlayıp oltalama saldırısı (Phishing attack) ile müşterinin ilgisini çekmeye çalışır ve müşteri gelip m-kuponu elde etmeye çalışırken saldırgan bilgileri kaydeder.

Ayrıca bunlara ek olarak burada daha büyük bir tehlike bulunmaktadır. Eğer saldırgan gelen tüm m-kupon taleplerini dinlemeyi başarırsa (müşteri ile kupon sağlayıcı arasındaki iletişime müdahale etmesine gerek yok), saldırgan m-kupon talep eden tüm müşterilerin MUC değerlerini elde edebilir. Tüm MUC değerlerini elde ettikten sonra da ister kendisi daha sonra kullanabilir isterse de üçüncü şahıslara satarak bundan kazanç sağlayabilir.

2.2.1.2. Kuponun oluşturulması aşamasındaki güvenlik açığı için çözüm önerisi

Tespit edilen açığı gidermek için MM Eşitlik (2.5) ile gönderilen veriyi göndermeden önce P'nin açık anahtarı ile şifrelemelidir Eşitlik (2.6). Ayrıca gerekli olmamakla birlikte ilave güvenlik için Şekil 2.4 ikinci adımda MM'e gönderilen SN değeri de MM'in açık anahtarı ile şifrelenebilir Eşitlik (2.7).

$$E(E(MUC \,||\, C, KR_{MM}), KU_P) \tag{2.6}$$

$$E(SN, KU_{MM}) \tag{2.7}$$

Mobil teknolojiler çok hızlı gelişmekte/ilerlemekte, bu kapsamda cihazların hesaplama kapasiteleri ve pil dayanıklılık süreleri de artmaktadır. Dolayısıyla algoritmanın ilk adımına yapılan açık anahtarlı şifreleme işlemi eklenmesi CPU ve pil kullanımını arttıracak olmasına rağmen, Hsueh ve Chen'in algoritmalarını (Hsueh ve Chen, 2010) sunmuş olduğu 2010 yılına nazaran sistemin genel kullanıma hiç etkisi olmayacak veya göz ardı edilebilir düzeyde olacaktır.

2.2.2. Kuponun kullanımı aşamasının güvenlik analizi

Bu aşamada MM göndermiş olduğu m-kupon bilgisinin doğru kasiyere (R) gittiğinden emin olabilmek için R'ye göndereceği mesaja (R_{ID}) mobil cihazını tanımlama bilgisini (MUC) ve R'nin kimlik bilgisini (ID_R) eklemektedir (Şekil 2.3).

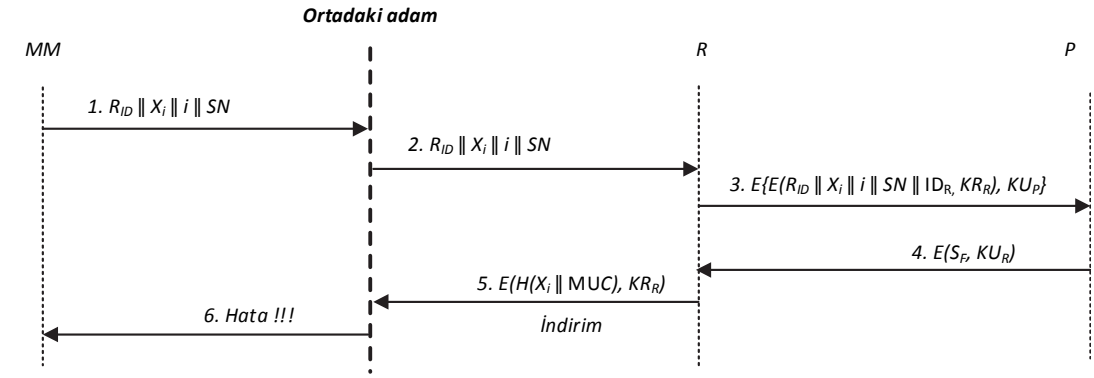
Algoritmada, MM'in ID_R bilgisini nasıl elde ettiği konusunda herhangi bir bilgi bulunmamaktadır. Bu nedenle ID_R bilgisinin elde edilmesi için iki yöntemin olduğu değerlendirilmiştir. Birinci yöntemde MM tüm ID_R bilgilerini zaten bilmektedir. İkinci yöntemde ise MM, ID_R bilgisini kuponun kullanılması aşamasında elde etmektedir. Bu iki yöntem içerisinde birinci yöntemin işletilmesi, listenin sürekli güncel olarak tutulması, sisteme eklenecek olan yeni satıcıların listeye nasıl ekleneceği gibi sorunlar nedeniyle işletilmesinin zor olacağı değerlendirilmektedir. Bu nedenle, her ne kadar algoritmada gösterilmese bile, ID_R bilgisinin ikinci metot olan kuponun kullanılması aşamasında elde edildiği kabul edilmiştir.

2.2.2.1. Senaryo I: Dışarıdan gelen röle saldırısı

Algoritmadaki zayıflık kasiyerin/satıcının ID_R bilgisinin alınmasında ortaya çıkmaktadır. Bu kısımda röle saldırısının (relay attack) kuponun kullanılması aşamasında nasıl yapıldığı anlatılmıştır. Saldırgan (ortadaki adam) MM ve R arasında yapılan iletişime müdahale eder Şekil 2.5 ve iletişimi kontrol eder. Saldırgan MM'den gelen ilk mesajı sanki mesajı gönderen kendisiymiş gibi R'ye iletir. Saldırganın paketin içeriğini bilmesine gerek yoktur. Mesajı alan R, algoritmayı normal bir şekilde yürütecek, normalde ne yapıyorsa aynı işlemleri yapacaktır. R mesajı kendi gizli anahtarı ile imzalayacak, sonrasında P'nin açık anahtarı ile şifrelediği mesajı P'ye gönderecektir. P gelen mesajı inceleyecek ve herhangi bir şeyden şüphelenmeyeceği için algoritmayı yürütmeye devam edecektir. P Eşitlik (2.8) ile gösterilen mesajı R'ye gönderecektir.

R normal olarak algoritmadaki rolü doğrultusunda Eşitlik (2.3)'ü gönderecektir. Tam da bu noktada saldırgan devreye girerek iletişime müdahale eder, R'den gelen indirimi alıp asıl müşteriye de işlem esnasında bir hata olduğunu ve işlemin gerçekleştirilemediğini, tekrar denemesi gerektiğini gösteren bir hata kodu gönderir. Bu noktadan sonra saldırgan devreden çıkarak iletişime müdahale etmeyi bırakır.

MM indirimi alabilmek için işlemi tekrar ettiğinde ise MM kuponun zaten kullanılmış olduğunu öğrenecektir. Bu sonucu alan asıl müşteri istemiş olduğu ürünü almaktan vazgeçebilir veya indirimsiz olarak almayı da tercih edebilir. Ayrıca MM bu durumla ilgili şikayette bulunsa bile bir sonuç elde edemeyecektir. Çünkü kayıtlar üzerinde yapılan inceleme sonucunda tüm işlemlerin MM tarafından yapıldığı sonucuna ulaşılacaktır.



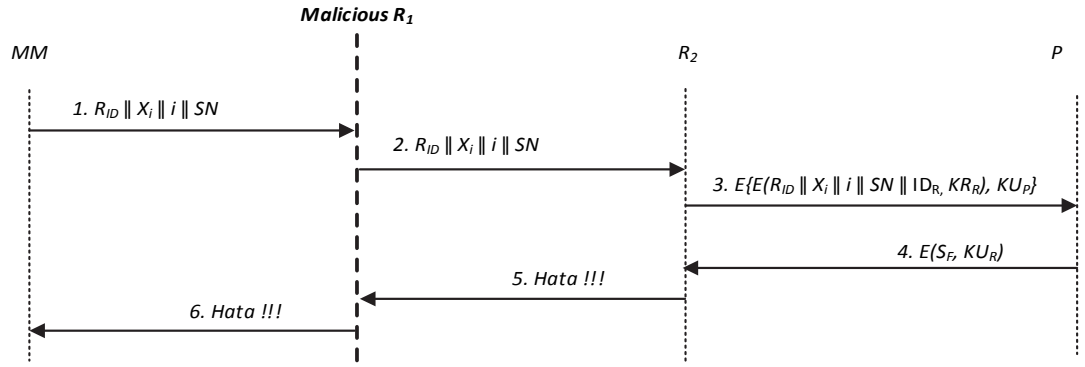
Şekil 2.5. Kuponun kullanılması aşamasında Ortadaki Adam Saldırısı

$$E(S_F, KU_R) \tag{2.8}$$

Bu saldırıda tek bir eksiklik bulunmaktadır. O da eğer tüm süreç NFC kullanılarak gerçekleştirilirse bu atak teorik olarak mümkün ancak pratik olarak uygulanabilir olmayacaktır. Çünkü NFC teknolojisi müşterinin ve satıcının cihazlarının birbirlerine çok yakın olmasını gerektirmektedir. Dolayısıyla saldırganın hem MM'e hem de R'ye görünmeden iletişime müdahale etmesi mümkün olmayacaktır. Sonuç olarak bu saldırıyı önlemek için yapılacak olan önlem tüm sürecin Wi-Fi, Bluetooth veya infrared teknolojisi ile değil NFC teknolojisi kullanılarak gerçekleştirilmesidir. Durum her ne kadar bu şekilde olsa da hala algoritmaya yapılabilecek başka bir saldırı bulunmaktadır.

2.2.2.2. Senaryo II: İçeriden yapılan röle saldırısı I – saldırgan kasiyerin (R) kendisi ise

Bu senaryoda R tüm saldırıyı kendisi yönetmektedir. Saldırı Şekil 2.6'da verilmiştir. Bu saldırı içeriden yapılan röle saldırısı olarak isimlendirilebilir.



Şekil 2.6. Kuponun kullanılması aşamasında içeriden yapılan role saldırısı-I

Saldırıyı R kendisi yapmaktadır. Bu nedenle saldırıda rol alan kasiyer Malicious R_1 olarak isimlendirilmiştir. Malicious R_1'in iletişimi dinlemesine gerek yoktur. Çünkü MM doğrudan Malicious R_1 ile temas kurmaktadır (Malicious R_1 ve R_2 satıcının (R) kasiyerleri olup saldırıda ikisi de yer almaktadır). MM kuponu kullanmak için indirim talebini kasiyere normal olarak gönderir. Malicious R_1 gelen mesajı, üzerinde hiçbir işlem yapmadan, R_2'ye yönlendirir. R_2 gelen mesaj sanki MM'den gelmiş gibi işlem yapar. Gelen mesajı önce kendi gizli anahtarı, sonra da P'nin açık anahtarı ile şifreleyerek P'ye gönderir. P gelen mesaj üzerinde yapacağı kontroller sonucunda herhangi bir şüpheli/hatalı işlem bulamayacaktır. Çünkü P'ye göre işlemler bir saldırgan tarafından değil, algoritmanın kullanıcıları olan MM ve R tarafından gerçekleştirilmektedir. P Eşitlik (2.8)'i hesaplayıp R_2'ye gönderecektir. Bu noktada R_2 saldırıyı gerçekleştirerek indirimi alacak, sonrasında da Malicious R_1'e hata mesajı gönderecektir. Hata mesajını alan MM işlemi tekrar deneyecek ancak bu sefer de kuponun zaten kullanıldığı mesajını alacaktır. Ya da Malicious R_1 müşteriye hiç detay vermeden sadece talep edilen kuponun geçersiz olduğunu da bildirebilir.

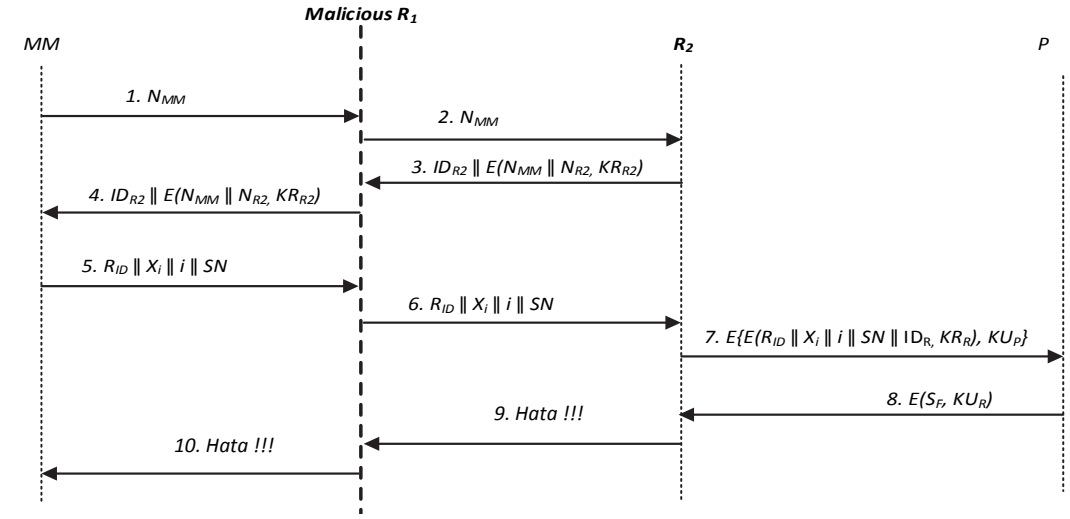
Saldırıda görüleceği üzere satıcı müşteriyi aldatmakta, müşteri ürünü ister indirimsiz fiyatıyla alsın ister almasın, indirimi kullanılmış gibi göstermektedir. R artık yapmış olduğunu iddia ettiği bu indirimi F'den almak için yapılan indirimin geri alınması sürecini başlatabilir.

2.2.2.3. Senaryo III: İçeriden yapılan röle saldırısı II – açık bir konu

İçeriden yapılan röle saldırısı MM, R ve P'nin kimlik bilgilerinin sürece eklenmesi ile de önlenemez. MM ile R arasında yapılan iletişim ISO kimlik doğrulama

standardı (ISO/IEC, 1993) kullanılarak yapılsa bile saldırı hala geçerlidir. Burada Malicious R_1'in yapması gereken sadece kimlik bilgisi olarak kendi bilgileri yerine MM'e R_2'nin bilgilerini göndermektir (burada saldırgan zaten R olduğu için kime hangi bilgiyi göndereceğini kendisi seçebilir). Saldırı Şekil 2.7'de gösterilmiştir.

Burada da görüleceği üzere saldırı içeriden geliyorsa MM'in bunu anlaması mümkün olmayacak, kupon sağlayıcı da aldatmayı anlamayacak ve R'nin kendisine göndermiş olduğu indirim talebinin doğru olduğunu onaylayacaktır. Ayrıca müşteri bu durumla ilgili şikayette bulunsa bile, tüm işlemler algoritmaya göre yapıldığı için, sonuç değişmeyecektir.



Şekil 2.7. Kuponun kullanılması aşamasında içeriden yapılan role saldırısı-II

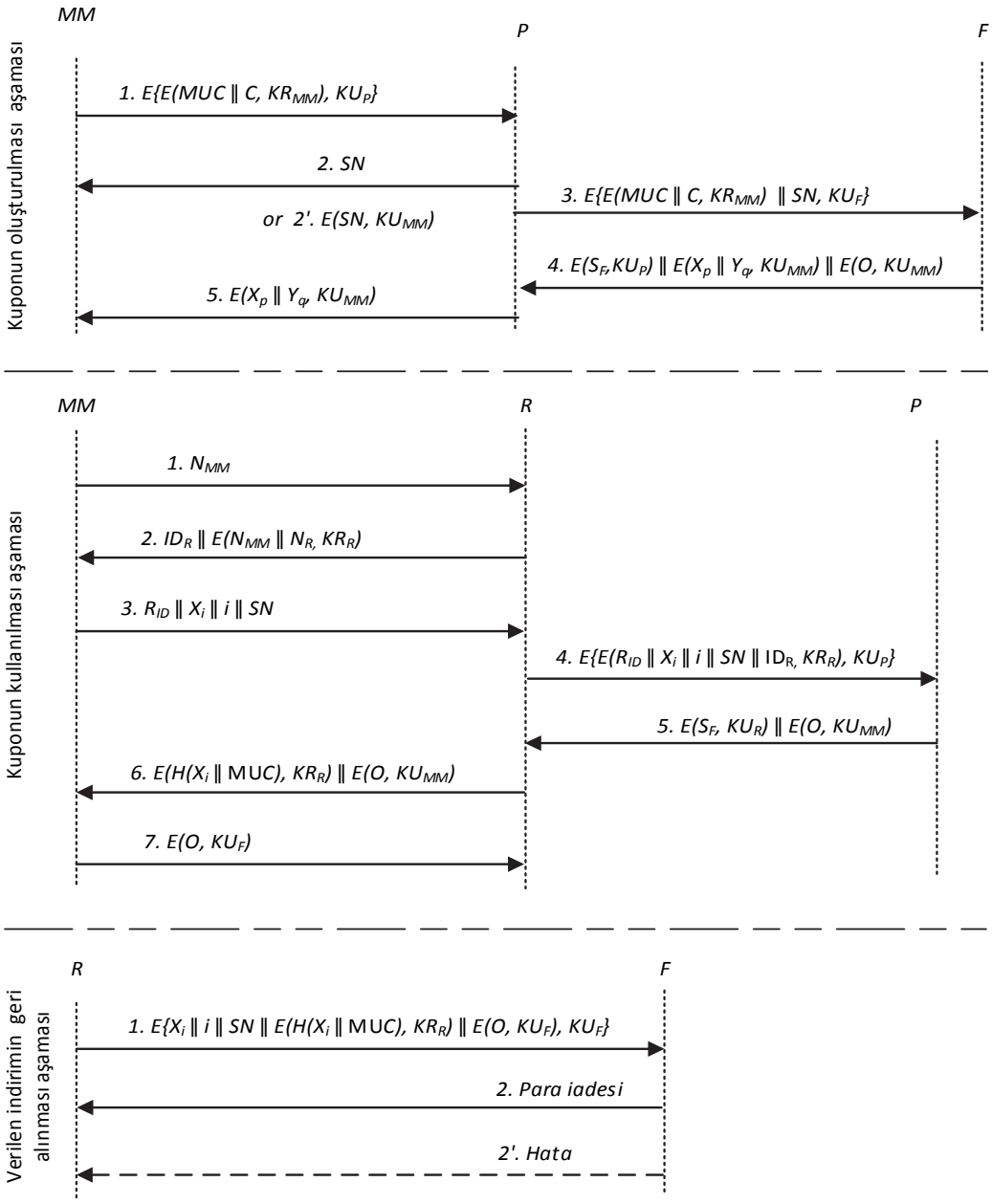
2.2.2.4. Röle saldırısı için çözüm önerisi

Bu saldırıyı önlemek ve asıl müşterinin indirimi aldığını garanti altına almak için algoritmaya onay kodu (O) ekledik. O değerini F belirlemekte ve sadece MM'in erişimine olanak sağlamak için MM'in açık anahtarı ile şifrelemektedir. Yapılan bu işlem ile MM kendisine sunulan indirimi aldığını ve sürecin başarılı bir şekilde tamamlandığını O değerini F'ye göndererek bildirebilir. İşlem basamakları Şekil 2.8'de verilmiştir. Süreç şu şekilde ilerlemektedir:

Kuponun oluşturulması aşamasının dördüncü adımında (Şekil 2.8) F onay kodu olarak kullanılacak olan O değerini belirler ve MM'in açık anahtarı ile şifreleyerek P'ye gönderir. P bu değeri kuponun kullanılması aşamasına kadar tutacaktır.

Kuponun kullanılması aşamasının beşinci adımında P Eşitlik (2.8) ve Eşitlik (2.9)'u R'ye gönderecektir.

$$E(O, KU_{MM}) \tag{2.9}$$



Şekil 2.8. Röle saldırısının onay kodu kullanılarak önlenmesi

Kuponun kullanılması aşamasının altıncı adımında Eşitlik (2.8) ve Eşitlik (2.9) ile gönderilen değerleri alan R, Eşitlik (2.9) ve Eşitlik (2.3) değerlerini MM'e gönderecektir. R'den gelen bu değerleri alan MM ilk önce Eşitlik (2.3) ile gelen değerleri kontrol edecektir. Eğer kontrol sürecinde sorun çıkmazsa MM Eşitlik (2.9)

ile gönderilen değeri kendi gizli anahtarı ile çözerek O değerini elde edecektir. Bu işlemden sonra MM indirimi başarılı bir şekilde aldığını bildirmek için O değerini F'nin açık anahtarı ile şifreleyerek R'ye gönderir. Böylelikle verilen indirimin geri alınması aşamasında F, indirimin gerçekten MM tarafından alındığını kontrol edebilecektir.

Bu adımla birlikte kuponun kullanılması aşaması tamamlanmış olmaktadır. R yapmış olduğu indirimi F'den geri alabilmek için indirimin geri alınması sürecini başlatacaktır. Algoritmaya yapılan onay kodu eklemesiyle R artık röle saldırısını gerçekleştiremeyecektir. Çünkü O değeri F'den MM'e gönderilmekte, bu değeri sadece MM açabilmekte, kuponu kullandığını göstermek için de MM bu değeri F'nin açık anahtarıyla tekrar şifreleyerek R'ye göndermektedir. Bu nedenle R indirimi geri alabilmek için Eşitlik (2.10) ve Eşitlik (2.11) ile gösterilen bilgileri F'ye gönderecektir.

$$E(O, KU_F) \tag{2.10}$$

$$E(X_i \,||\, i \,||\, SN \,||\, E(H(X_i \,||\, MUC), KR_R) \,||\, E(O, KU_F), KU_F) \tag{2.11}$$

R'nin göndermiş olduğu mesajları alan F gelen değerleri kontrol edecektir. Bu kapsamda Eşitlik (2.11) ile gelen veriyi çözerek O değerini kontrol eder. Eğer gelen O' değeri ile kendisinin göndermiş olduğu O değerleri aynı ise MM'in indirimi gerçekten kullandığını anlayacak ve R'ye indirimi geri iade edecektir. Algoritmaya yapılan bu eklemeler ile birlikte röle saldırıları artık yapılamayacaktır.

2.3. Hesaplama Maliyeti

Hsueh ve Chen tarafından geliştirilen algoritmanın güvenlik incelemesinden sonra algoritmada zayıf noktaların olduğu tespit edildi ve bu açıkların giderilmesi için algoritmaya eklemeler yapılarak yeni bir algoritma önerildi. Fakat yapılan bu eklemelerin sisteme getireceği bir maliyet bulunmaktadır. Algoritmaya yapmış olduğumuz eklemelerin müşteriye (MM) getirmiş olduğu maliyet Tablo 2.1'de sunulmuştur. Yapılan maliyet analizi çalışmasında MM sadece kuponun oluşturulması ve kuponun kullanılması aşamalarında yer aldığı için bu iki kısım dikkate alınmıştır.

Tablo 2.1. MM'in dahil olduğu aşamaların maliyet analizi

	Hsueh ve Chen algoritması		**Önerilen yeni** algoritma	
Aşama	**İşlem**	**Adet**	**Ek işlem**	**Adet**
Kuponun oluşturulması aşaması	İmzalama Şifre çözme	1 1	Şifreleme	1
Kuponun kullanılması aşaması	Özet fonksiyonu Doğrulama	1 1	Şifre çözme Şifreleme	1 1

Kuponun oluşturulması aşamasında tespit edilen açığı önlemek için Eşitlik (2.6) ile gösterilen adıma şifreleme eklenmiştir. Kuponun kullanılması aşamasındaki açığı gidermek ve röle saldırısını önlemek için algoritmaya bir onay kodu (O) eklenmiştir Eşitlik (2.9). Yapılan bu ekleme ile MM'in işlem yüküne bir şifreleme bir de şifre çözme adımı eklenmiş oldu. Algoritmaya yapılan açık anahtarlı şifreleme ve çözme işlemi her ne kadar CPU ve pil kullanımını arttıracak olsa da mobil cihazların teknolojik olarak çok hızlı gelişmeleri nedeniyle çözüm için önerilen yapının kolaylıkla uygulanabilir olduğunu söyleyebiliriz.

3. HSIANG M-KUPON ALGORİTMASI

3.1. Algoritmanın Genel Yapısı

Hsiang tarafından yapılan çalışmada (Hsiang, 2014) önerilen algoritmanın basit, güvenli ve sadece birkaç özet fonksiyonu kullanarak gerçekleştirildiği, bununla birlikte NFC teknolojisi kullanılarak oluşturulacak m-kuponlar için gerekli tüm güvenlik ihtiyaçlarının da karşılandığı ifade edilmektedir. Ayrıca, NFC teknolojisinin kablosuz bağlantı ile çalışması nedeniyle tek başına güvenli iletişimi sağlayamayacağı, gizlice dinleme (eavesdropping) saldırılarına karşı yeterli olmayacağı ve verilerin değiştirilmesini engelleyemeyeceği vurgulanmıştır. Dolayısıyla yeterince korunamayan bir m-kupon, çok az bir maliyet ve gayretle, kopyalama ve değiştirme saldırılarına açık hale gelmektedir.

Hsiang, önermiş olduğu algoritmanın yukarıda bahsedilen saldırılara karşı güvenli olduğunu belirtmektedir. Önerilen algoritmada kullanılan gizli anahtarın sadece kupon sağlayıcı ve kasiyer tarafından bilindiği, böylece sadece yetkilendirilmiş kupon sağlayıcının geçerli bir m-kupon üretebileceği ve gizli anahtarı bilen kasiyerin de kuponun geçerliliğini kontrol edebileceği belirtilmektedir. Algoritmada kasiyer ve kupon sağlayıcı aynı organizasyonun parçası olarak planlanmıştır. Yani kupon sağlayıcı ve kupondaki indirimi veren firma aynıdır. Öncelikle kullanıcı, m-kupon için kullanılacak olan programı mobil cihazına yüklemek zorundadır. Kasiyer ile tüm kupon sağlayıcıların (NFC Target) da gizli anahtar x ve kupon bilgilerinin bulunduğu Teklif''i paylaşmaları gerekmektedir. Böylelikle, kupon sağlayıcı tarafından oluşturulan kuponların geçerlilik kontrolünün kasiyer tarafından yapılabilmesi için bu değerler kullanılacaktır. Algoritma iki aşamadan oluşmaktadır: kuponun oluşturulması, kuponun kullanılması ve kimlik doğrulaması.

3.1.1. Kuponun Oluşturulması Aşaması

Müşteri m-kuponu almak için mobil cihazını NFC hedefine yaklaştırır ve ID_m ve PIN bilgilerini gönderir. Kupon sağlayıcı bu bilgileri aldıktan sonra rasgele bir sayı (S_f) üretir. Daha sonra kendi ID değerini (ID_f), üretmiş olduğu S_f ve müşterinin ID_m değerlerini kullanarak Eşitlik (3.1) ile a değerini hesaplar. Kupon sağlayıcı P değerini hesaplamak için, S_f ve PIN değerlerini sadece kendisi ve kasiyer tarafından bilinen x değeri ile XOR işlemine tabi tutar (Eşitlik (3.2)). Aslında burada Eşitlik (3.1) ve Eşitlik (3.2) ile yapılan işlemler, basit bir XOR ile simetrik şifreleme işlemidir. Daha sonra kupon sağlayıcı elde etmiş olduğu a ve S_f değerlerini açık anahtarlı şifreleme işlemine tabi tutarak A ve B değerlerini elde eder (Eşitlik (3.3) ve Eşitlik (3.4)). Müşteriye M_{kupon} bilgisini göndermeden önce rasgele sayı S_f ve Eşitlik (3.1) ile elde etmiş olduğu a değerlerini kullanarak K değerini hesaplar (Eşitlik (3.5)) ve hesapladığı değerleri müşteriye gönderir (Eşitlik (3.6)). Kuponun oluşturulması işlemleri Şekil 3.1'de ve kullanılan sembollerin anlamları simgeler ve kısaltmalar dizini altında gösterilmiştir.

$$a = h(ID_f) \oplus S_f \oplus ID_m \tag{3.1}$$

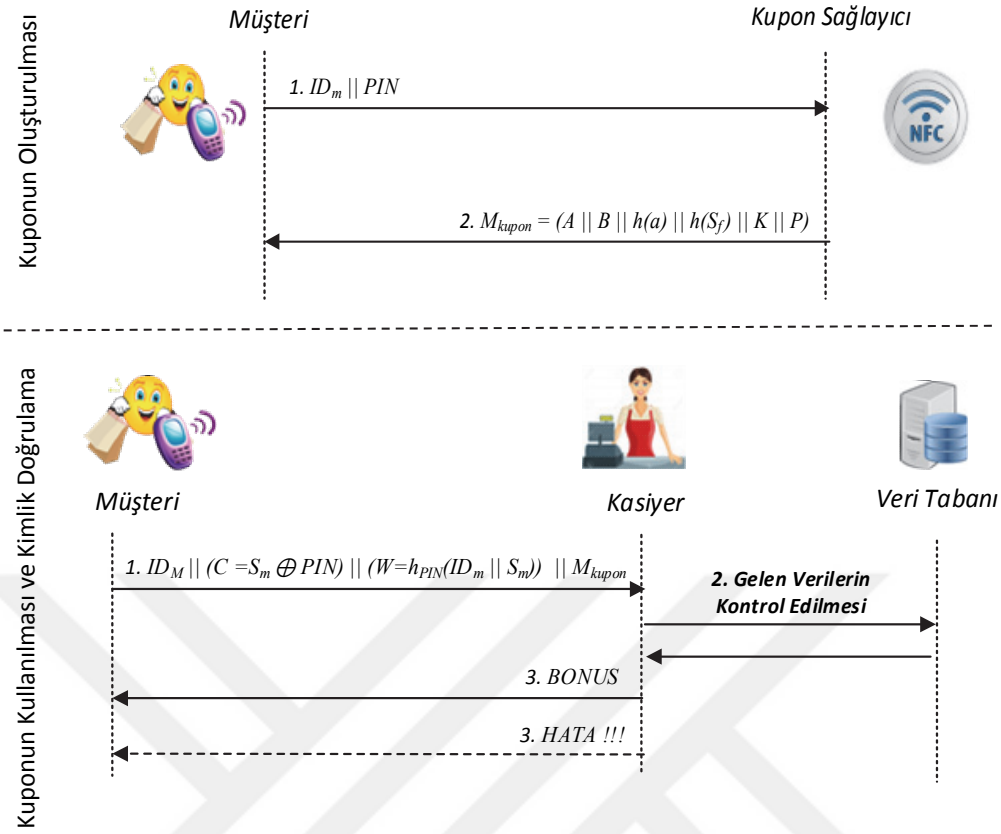
$$P = S_f \oplus x \oplus PIN \tag{3.2}$$

$$A = a^2 \bmod n \tag{3.3}$$

$$B = S_f^2 \bmod n \tag{3.4}$$

$$K = h_{Vf}(S_f \,||\, a) \tag{3.5}$$

$$M_{kupon} = (A \,||\, B \,||\, h(a) \,||\, h(S_f) \,||\, K \,||\, P) \tag{3.6}$$



Şekil 3.1. Hsiang m-kupon algoritması (Hsiang, 2014)

3.1.2. Kuponun kullanılması ve kimlik doğrulama

Müşteri m-kuponu kullanmak için, rasgele bir sayı (S_m) üretir. S_m ve ID_m değerlerini kullanarak Eşitlik (3.7) ve Eşitlik (3.8) ile C ve W değerlerini hesaplar. Bu değerler ile birlikte ID_m ve Eşitlik (3.6) ile hesaplanıp kendisine gönderilmiş olan M_{kupon} bilgilerini kasiyere gönderir. Kasiyer C, W, ID_m ve M_{kupon} bilgilerini aldıktan sonra veri tabanında ID_m değerini kullanarak kuponun daha önce kullanılıp kullanılmadığını kontrol eder. Kupon daha önce kullanılmamışsa (3.9)-(3.12) numaralı Eşitlikleri kullanarak W′ değerini hesaplar. Hesapladığı W′ değeri ile W değerini karşılaştırır. Eğer değerler farklı ise kupon reddedilir.

$$C = S_m \oplus PIN \tag{3.7}$$

$$W = h_{PIN}(ID_m \,||\, S_m) \tag{3.8}$$

$$S_f = h(ID_f) \oplus ID_m \oplus a \tag{3.9}$$

$$PIN = P \oplus S_f \oplus x \tag{3.10}$$

$$S_m = C \oplus PIN \tag{3.11}$$

$$W' = h_{PIN}(ID_m \,||\, S_m) \tag{3.12}$$

$$h(ID_f) = a \oplus S_f \oplus ID_m \tag{3.13}$$

$$V_f' = h_x(ID_f \,||\, Teklif) \tag{3.14}$$

$$K' = h_{Vf}'(S_f \,||\, a) \tag{3.15}$$

Kasiyer, Eşitlik (3.3) ve Eşitlik (3.4) ile yapılan açık anahtarlı şifreleme işlemini çözmek için Çin artık teoremini (Lady, Chinese remainder theorem) kullanır. Bunun için müşteriden gelen A ve B değerlerini kullanarak a ile S_f değerlerini tespit eder. Elde ettiği a değerini kullanarak S_f değerini hesaplar (Eşitlik (3.9)). Elde ettiği S_f değerini kullanarak müşterinin PIN değerini elde eder (Eşitlik (3.10)) ve müşterinin üretmiş olduğu S_m değerini Eşitlik (3.11) ile hesaplar. Kasiyer gelen verilerden elde etmiş olduğu değerleri kullanarak W′ değerini hesaplar (Eşitlik (3.12)). Hesapladığı W′ değeri ile müşterinin göndermiş oluğu W değeri aynı ise kasiyer $h(ID_f)$ değerini elde etmek için Eşitlik (3.13)'ü kullanır. Kasiyer elde ettiği $h(ID_f)$ değerini kullanarak veri tabanından kupon sağlayıcının (ID_f) verdiği kupon bilgilerini (Teklif) bulur. Sonrasında (3.14) ve (3.15) numaralı Eşitlikler ile K′ değerini hesaplar ve K değeri ile karşılaştırır. Elde ettiği ID_m ve Teklif bilgilerini kullanarak m-kuponun daha önce kullanılıp kullanılmadığını kontrol eder. Kupon geçerliyse bilgileri veri tabanına kaydeder ve müşteriye kuponda yer alan indirimi uygular. Yapılan bu işlemler sayesinde hem müşterinin bilgileri kontrol edilerek kimlik doğrulama yapılmış hem de veri tabanı üzerinde kuponun daha önce kullanılıp kullanılmadığı kontrol edilmiştir. Kuponun kullanılması ve kimlik doğrulama işlemleri Şekil 3.1'de gösterilmiştir.

Hsiang tarafından NFC teknolojisinin, iletişimi gizlice dinleme ve içeriği değiştirme (modification) saldırılarına karşı tek başına güvenlik sağlayamadığı, bu kapsamda NFC cihazları ile yapılan iletişimin güvenli bir kanal üzerinden yapılmasının en iyi yaklaşım olacağı belirtilmiştir.

Önerilen algoritmada, kasiyer ve kupon sağlayıcılar arasında gizli bir anahtar (V_f) paylaşıldığı, güvenli kanal üzerinden aralarında yapılan veri iletişiminde bu anahtarın kullanıldığı, böylelikle gizlilik, bütünlük ve kimlik doğrulamanın sağlanıldığı, A, B, h(a), h(S_f) değerlerinin kuadratik varsayım (quadratic assumption) üzerine hesaplandığı, dolayısıyla $A = a^2 \bmod n$ eşitliğinde kullanılan a değerinin p, q ve n değerleri bilinmeden bulunabilmesinin matematiksel olarak mümkün olmadığı, algoritmanın yeniden gönderme saldırısı (replay attack), kupon kopyalama/çoğaltma, kuponun çoklu kullanımı, yetkisiz kupon üretme ve veri değiştirme ataklarına karşı dayanıklı olduğu belirtilmiştir. Burada $A = a^2 \bmod n$ eşitliği ile yapılan işlem açık anahtarlı şifreleme işlemidir (a değerinin şifrelenerek A değerinin elde edilmesi). Bu eşitlikte yer alan a'nın üssü olan 2 (e = 2) ve n değerleri açık anahtar çiftini ifade etmektedir. p ve q değerleri ise çok büyük asal sayıları ifade etmekte olup bu değerler n değerinin (n = p x q) elde edilmesinde kullanılan gizli anahtarlardır. Burada yapılan işlemde yer alan n değeri her ne kadar açık anahtarın bir parçası olsa da bu değer de algoritmada gizli tutulmakta ve müşteri tarafından bilinmemektedir. Dolasıyla saldırganın elinde hem gizli anahtarlar hem de açık anahtarlardan birisi bulunmamakta, çok büyük sayıların çarpanlarına ayrılması probleminin zorluğu nedeniyle de p, q ve n değerleri bilinmeden a değerinin matematiksel olarak hesaplanması mümkün olmamaktadır (Montgomery, 1994).

3.2. Algoritmanın Güvenlik Analizi

Güvenlik analizi için algoritmaya, kuponların çoklu kullanımı, yeniden gönderme, müşterinin kimlik bilgilerinin çalınması, yetkisiz kupon kullanma/üretme, kuponun geçersiz hale getirilmesi, gizli anahtarın elde edilmesi saldırıları yapılmış, saldırganın elde ettiği paketleri çözüp çözemediği, sistemi manipüle edip edemediği incelenmiştir. Senaryoda müşteri, kupon sağlayıcı ve kasiyer sürecin doğal üyesi olarak bulunmaktadır. Güvenlik analizi için saldırgan, kimi zaman iletişimi sadece dinlemiş (eavesdropping), kimi zaman da aktif rol alarak iletişime müdahale (man-in-the-middle attack) etmiştir. Elde edilen veriler doğrultusunda sonuçlar iki kısma ayrılmıştır. Birinci kısımda algoritmanın güçlü kısımları, ikinci kısımda ise güvenlik açıkları gösterilmiştir.

3.2.1. Algoritmanın güçlü kısımları

Öncelikle algoritma, tüm süreci firmanın kendisinin yönetmesi üzerine kurulmuştur. Firma kendi indirimlerini belirlemekte, kuponları üretmekte, müşteriye dağıtmakta ve sonrasında indirimi müşteriye kullandırmaktadır. Algoritmanın dayanıklı olduğu belli başlı ataklar; ortadaki adam saldırısı (kuponun kullanımı aşamasında), kuponların çoklu kullanım saldırısı ve yeniden gönderme saldırısıdır. Bu saldırıların detayları aşağıda sunulmuştur:

3.2.1.1. Ortadaki adam saldırısı

Sıfır toplamı modeli doğrultusunda yapılan simülasyon ile ilk saldırı olarak ortadaki adam saldırısı denenmiştir. Bu saldırı senaryosu, kuponun elde edilmesi aşaması, kuponun kullanılması aşaması ve kuponun kontrol edilmesi aşamalarında ayrı ayrı uygulanmıştır. Tüm sürecin aynı firma tarafından kontrol edilmesi sayesinde firma kendi güvenliğini kendisi sağlama fırsatı yakalamaktadır. Özellikle kupon sağlayıcı ile kasiyerin aynı firmanın parçası olması nedeniyle kupon sağlayıcı ve kasiyer arasındaki iletişimin ortadaki adam saldırılarına maruz kalma ihtimali ortadan kalkmakta, böylelikle sistem, kuponun kullanılması aşamasında bu saldırıdan kurtulmaktadır.

Ayrıca algoritmanın NFC tabanlı olması nedeniyle kuponun kullanılması aşamasında saldırganın (müşterinin kendisi saldırgan olmamak kaydıyla) fiziksel olarak müşteri ile kasiyer arasına fark edilmeden girmesi ve iletişime müdahale etmesi mümkün değildir.

3.2.1.2. Kuponların çoklu kullanımı saldırısı

Bu saldırı için iki ayrı senaryo planlanmıştır. İlk senaryoda saldırganın dışarıdan birisi olması durumu ele alınmış, ikinci senaryoda müşterinin kendisi saldırgan olarak davranmıştır. Senaryoda saldırgan/müşteri kuponu kullanma aşamasında kuponu tekrar kullanmak için kasiyere göndermektedir. Ancak, kuponun her oluşturuluşunda (her işlem için) yeni bir rasgele sayı (S_f) üretilmekte, bu değer Eşitlik (3.1) ile elde edilen a değerinin hesaplanmasında ve sonrasında kuponun kullanımı aşamasında kontrol değeri olarak kullanılmaktadır. Ayrıca kuponların

kullanım bilgileri veri tabanına kaydedilmektedir. Bu sayede saldırgan/müşteri herhangi bir kupon kullanımı talebinde bulunduğunda, veri tabanı kontrol edilerek kuponun daha önceden kullanılıp kullanılmadığı kontrol edilmektedir. Eğer kupon veri tabanında kayıtlı ise işlem sonlandırılmaktadır.

3.2.1.3. Yeniden gönderme saldırısı

Yeniden gönderme saldırısı yöntem ve senaryo olarak kuponların çoklu kullanımı saldırısına benzemektedir. Bu senaryoda saldırgan, kuponların çoklu kullanımı saldırısında olduğu gibi, kasiyere paketleri tekrar göndermektedir. Ancak gönderilen tüm paketler orijinal/geçerli olsalar dahi, kullanılan tüm kuponlar veri tabanına kaydedildiği için saldırı başarısız olmaktadır.

3.2.2. Algoritmanın zayıf kısımları

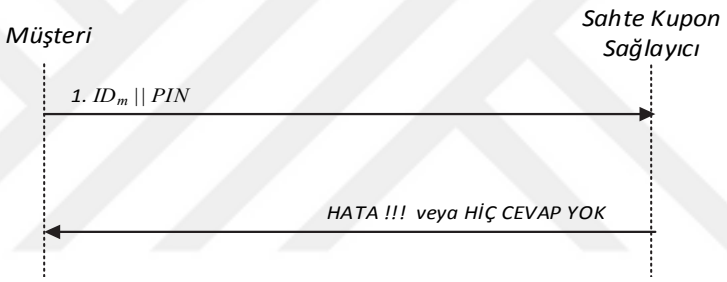
Tüm sürecin firmanın kendisi tarafından yönetilmesi algoritma için artı bir özellik olsa da aynı zamanda bazı yöntemlerin kullanılmasını engellemektedir. Örneğin, farklı firmalara ait indirim kuponlarının tek bir noktadan dağıtılmasını sağlayan, özel indirimler sunan web siteleri/portallar giderek yaygınlaşmakta, bu tarz sitelerin kullanılması bu yöntemde mümkün olmamaktadır. Bu portal/sitelerin kupon kullanımına etkileri ile ilgili yapılan çalışmalar (Haraniya, 2017; Reinhart ve Naatus, 2017) müşterilerin bu tarz siteleri kullanmayı tercih ettiklerini göstermektedir.

Ayrıca, eğer firmanın birden fazla şubesi var ise bu algoritmayı kullanabilmesi için merkezi bir veri tabanı sistemi kurması gerekecektir. Böyle bir durumda da şubedeki kasiyer ile merkezi veri tabanı arasında kurulacak olan iletişim için Ortadaki Adam Saldırısı yapılabilir olacaktır. Algoritmaya uygulanabilecek saldırı senaryoları aşağıda alt başlıklarda sunulmuştur.

3.2.2.1. Müşterinin kimlik bilgilerinin çalınması

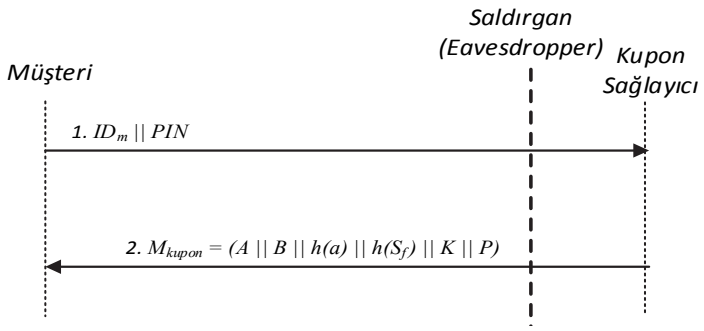
Bu saldırı senaryosu müşterinin indirim kuponunu ilk alacağı/oluşturulacağı zamanı kapsamaktadır. Senaryoda saldırı sahte bir kupon sağlayıcı ile (Oltalama Saldırısı - Phishing) (Şekil 3.2) veya var olan bir kupon sağlayıcının önüne bir pasif NFC okuyucu konulması şeklinde (iletişimi gizlice dinleme) (Şekil 3.3) planlanmıştır.

Senaryoda firma, kuponların dağıtımını NFC özellikli posterler aracılığı ile yapmaktadır. Saldırgan fiziksel olarak aynı görünümlü bir poster üreterek müşterilerin ilgisini çekmeye çalışmakta veya çok basit olarak NFC okuyucu özelliği olan bir okuyucuyu posterin üzerine yapıştırıp müşterinin indirim kuponunu normal olarak almasını beklemektedir. Şekil 3.2'de gösterilen saldırıda müşteri saldırganın yerleştirdiği sahte kupon üzerinden m-kuponu normal bir şekilde almaya çalışmakta, ID_m ve PIN değerlerini saldırgana göndermektedir. Müşteri kupon bilgilerini beklerken saldırgan gelen verileri kaydetmekte, müşteri ise herhangi bir veri/sonuç elde edememektedir. Şekil 3.3'te gösterilen saldırıda ise saldırgan, müşteriye sunulan normal bir m-kupon posterinin üzerine bir NFC okuyucu yerleştirmekte, müşteri talep ettiği m-kuponu sorunsuz olarak alırken saldırgan da aradaki trafiği kaydetmektedir.



Şekil 3.2. Kuponun elde edilmesi aşamasında oltalama

Saldırgan yerleştirmiş olduğu "sahte kupon sağlayıcı" ile veya iletişimi dinleyerek müşteriye ait ID_m ve PIN değerlerini elde etmiş ve böylece o müşteri gibi hareket edebilme olanağına kavuşmuştur (impersonation attack). Çünkü müşteri, sadece bu değerlere göre kontrol edilmektedir. Saldırı için yapılan simülasyonun akış diyagramı ve sözde kodları Ek-A'da verilmiştir.



Şekil 3.3. Kuponun elde edilmesi aşamasında iletişimi dinleme

3.2.2.2. Yetkisiz kupon kullanma/üretme

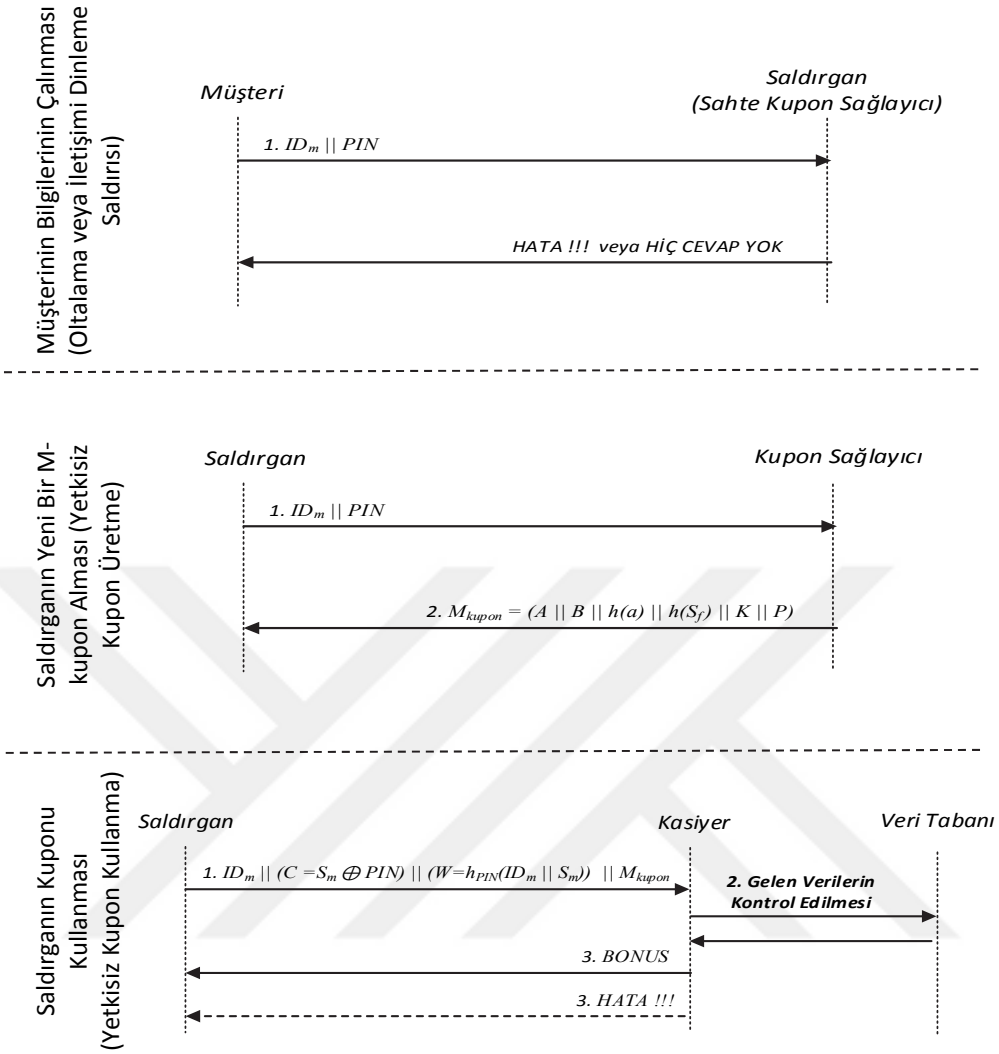
ID_m ve PIN değerlerini elde eden saldırgan, gerçek müşterinin yerine geçme ve geçerli bir kupon elde etme şansına sahip olmuştur. Bu saldırı özellikle özel müşterilere özel olarak tanımlanan indirimlerin kullandırılmasında soruna neden olur. Örneğin, sürekli alışveriş yapan müşterilere belirli bir süreliğine aldığı ürünlerde ekstra indirim sağlandığını varsayalım. Bu indirimin sadece o müşteri/müşteriler tarafından kullanılması gerekir ki indirim hedefine ulaşsın. Aksi takdirde başka birisinin kullanması hem firmaya ekonomik olarak zarar verir hem de müşterinin firmayla olan bağını zedeleyebilir.

Şekil 3.4'te gösterilen saldırı şu adımlardan oluşmaktadır:

1. Saldırgan ilk olarak kuponun oluşturulması aşamasında müşterinin ID_m ve PIN değerlerini oltalama saldırısı ile elde eder (Şekil 3.4 birinci kısım).

2. Elde ettiği bu değerleri kullanarak normal bir müşteri gibi kupon sağlayıcıdan yeni bir m-kupon talep eder ve alır (Şekil 3.4 ikinci kısım).

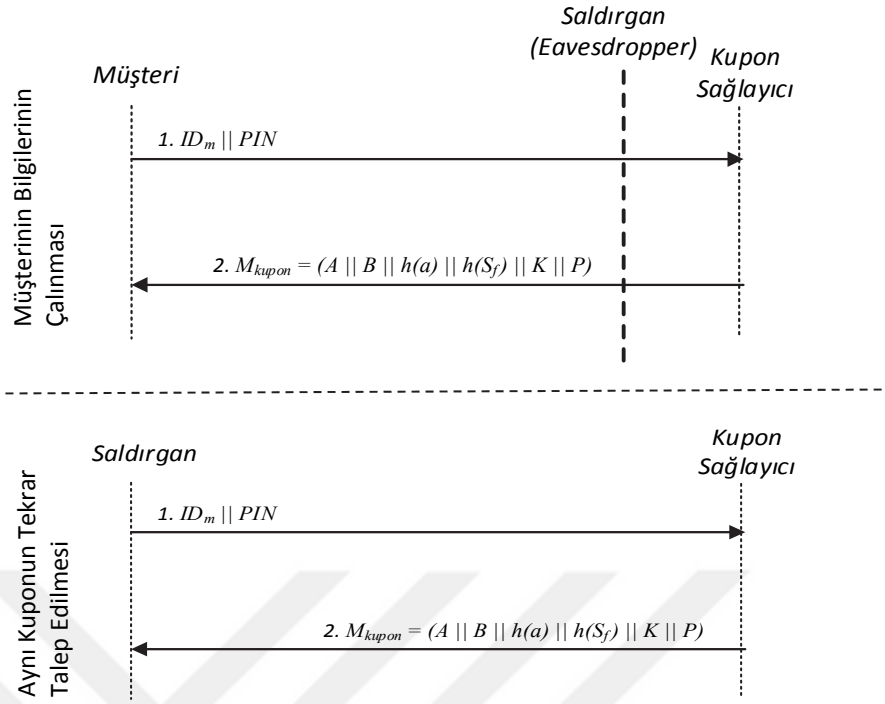
3. Daha sonra elde ettiği kuponu kullanmak için kasiyere götürür ve istemiş olduğu indirimi gerçek müşterinin yerine alır (Şekil 3.4 üçüncü kısım). Saldırı için yapılan simülasyonun akış diyagramı ve sözde kodları Ek-A'da verilmiştir.



Şekil 3.4. Saldırganın kuponu elde etmesi ve kullanması

3.2.2.3. Kuponun geçersiz hale getirilmesi saldırısı

Müşterinin ID_m ve PIN değerlerini ele geçirmesi, bu değerleri kullanarak başka bir müşteri adına oluşturulan kuponları kullanması ve bu şekilde firmayı ekonomik zarara uğratması firmanın büyüklüğüne göre önemsiz gibi görünebilir. Ancak burada unutulmaması gereken nokta, indirimin başka bir kişi tarafından kullanılabildiği gerçeğidir. Bahsedilen saldırı her ne kadar ekonomik olarak önemsiz gibi görünse de altında firmaya verilebilecek ciddi bir imaj zararı barındırmaktadır. Şöyle ki; saldırgan müşterinin kimlik bilgilerini kullanarak kendisine yeni kuponlar oluşturmak yerine firmanın doğrudan imajına ve güvenirliliğine zarar vermek için farklı bir yöntem izleyebilir. Saldırgan, müşterinin almış olduğu kuponu geçersiz hale getirebilir.



Şekil 3.5. M-kuponun geçersiz hale getirilmesi

Şekil 3.5'te gösterilen saldırı şu adımlardan oluşmaktadır:

1. Saldırgan ilk olarak kuponun oluşturulması aşamasında müşterinin ID_m ve PIN değerlerini oltalama saldırısı veya iletişimi dinleme yöntemi ile elde eder. Burada saldırgan müşteriye ait bilgileri daha önce de elde etmiş olabilir. Saldırı için uygun bir an kollayıp sonra da saldırıyı gerçekleştirebilir.

2. Müşteri normal bir şekilde m-kuponunu elde eder.
3. Müşteri aldığı kuponu kullanmak üzere kasiyere giderken saldırgan devreye girer ve atak başlar.
4. Saldırgan ID_m ve PIN değerlerini kullanarak aynı m-kuponu yeniden talep eder. Kupon sağlayıcı da aynı kuponu tekrar üreterek saldırgana gönderir. Kupon sağlayıcı burada herhangi bir kontrol yapmadığı için müşterinin başka birisi olup olmadığını anlayamaz ve kuponun daha önce verilip verilmediğine bakmadan yeni bir S_f değeri üretir. S_f değeri yeniden üretildiği için a, P, A, B ve K değerleri komple değişmiş olur. Böylece m-kupon yeniden üretilmiş ve eski m-kupon geçersiz hale gelmiş ve saldırı başarılı olmuştur.

Hiçbir şeyden haberi olmayan müşteri kasiyere gidip kuponu kullanmak istediğinde kuponunun geçersiz olduğunu öğrenir ki bu istenilmeyen bir durumdur. Bu saldırı doğrudan firmanın güvenirliliğine yönelik yapılmaktadır. Aldığı kuponun geçersiz olduğunu öğrenen müşteri bunu başka müşterilerle de paylaşacağı için firmanın imajı olumsuz etkilenecektir. Dolayısıyla bu saldırı etki olarak bir önceki saldırıdan çok daha güçlüdür.

3.2.2.4. Gizli anahtarın elde edilmesi saldırısı

Hsiang, önermiş olduğu algoritmanın yapılacak saldırılara karşı güvenli olduğunu, saldırganın istese de m-kupon bilgisini M_{kupon} = (A || B || h(a) || h(S_f) || K || P) çözemeyeceğini, Eşitlik (3.1) ile hesaplanan a değerinin geri hesaplanmasının matematiksel olarak uygulanabilir olmadığını (computationally infeasible) belirtmiştir. Hatta saldırganın a ve S_f değerlerini bir şekilde elde ettiği varsayılsa bile ID_f değerinin elde edilemeyeceğini, böylece de algoritmanın kupon sağlayıcının ID'sinin gizliliğini sağlayacağını iddia etmiştir.

Ancak, yapmış olduğumuz çalışmada burada gözden kaçan bir nokta olduğunu tespit ettik. Algoritma, iddia edildiği gibi kupon sağlayıcının ID'sinin gizliliğini sağlasa da saldırgan, a ve S_f değerlerini kullanarak, kupon sağlayıcının kendi içinde yapmış olduğu haberleşmede kullandığı sabit gizli anahtarı (x) elde edebilmektedir. Saldırı şu şekilde yapılmıştır:

1. Saldırgan "Müşterinin Bilgilerinin Çalınması Saldırısı"nı gerçekleştirerek müşterinin ID_m ve PIN değerlerini elde eder.
2. Ardından kupon sağlayıcıya giderek herhangi bir m-kupon talebinde bulunur.
3. Kupon sağlayıcı saldırgana istemiş olduğu m-kuponu gönderir. Saldırgan kupon sağlayıcıdan gelen M_{kupon} bilgisini elde eder.
4. Artık saldırganın elinde ID_m, PIN, A, B, h(a), h(S_f), K, P, a ve S_f değerleri bulunmaktadır. Bu noktadan sonra saldırganın bilmediği değerler olarak sadece h(ID_f), x, V_f,, ID_f, ve Teklif değerleri kalmıştır.
5. Saldırgan ID_m, a ve S_f değerlerini kullanarak Eşitlik (3.13) ile h(ID_f) değerini elde eder.
6. Sonrasında PIN, P ve S_f değerlerini kullanarak x değerini elde eder (Eşitlik (3.16)). Algoritmada da bahsedildiği gibi x değeri kupon sağlayıcı, kasiyer ve

veri tabanı arasında kullanılan sabit gizli anahtardır, dolayısıyla saldırgan bu gizli anahtarı elde edebilmektedir.

$$x = P \oplus S_f \oplus PIN \tag{3.16}$$

Eşitlik (3.16) ile yapılan işlemle saldırgan artık gizli anahtara da sahiptir. Elinde olmayan değerler ise kasiyer ile veri tabanı arasındaki iletişimde kullanıldığı belirtilen Eşitlik (3.14) ve Eşitlik (3.15) ile hesaplama yöntemi gösterilen V_f , ID_f ve Teklif değerleridir.

Saldırı öncesinde saldırganın elinde bulunan bilgiler, saldırı sonrasında elde ettiği bilgiler ile saldırı sonrasında da elde edemediği bilgiler Tablo 3.1'de gösterilmiştir. Saldırgan, elde ettiği bu gizli anahtarla, kupon sağlayıcı ile veri tabanı ve/veya kasiyer ile veri tabanı arasındaki iletişimi bile çözümleyebilir. Ancak buna karar verebilmek için elimizde yeterli veri bulunmamaktadır. Çünkü bu iletişimin nasıl yapıldığına dair algoritmada herhangi bir bilgi bulunmamaktadır.

Tablo 3.1 Saldırı öncesi bilenen, saldırı sonrasında elde edilen değerler

Saldırıdan önce bilinen değerler	a, S_f
Saldırıdan önce bilinmeyen değerler	ID_m , PIN, A, B, h(a), h(S_f), K, P, h(ID_f), x, V_f, ID_f, Teklif
Saldırı sonucunda elde edilen değerler	ID_m , PIN, A, B, h(a), h(S_f), K, P, h(ID_f), x
Saldırı sonrasında da elde edilemeyen değerler	V_f, ID_f, Teklif

3.2.3. Saldırılara sunulan çözüm önerileri

3.2.3.1. Müşterinin kimlik bilgilerinin çalınması, yetkisiz kupon kullanma/üretme ve kuponun geçersiz kılınması saldırılarına çözüm önerisi

Hsiang tarafından geliştirilen algoritmada güvenlik kontrollerinin özellikle kuponun kullanımı aşamasına bırakılması, kuponun oluşturulması aşamasında herhangi bir kontrolün bulunmaması, güvenlik zafiyetine neden olmaktadır. Bu zafiyet kullanılarak yukarıda bahsedilen saldırılar gerçekleştirilebilmektedir.

Bu nedenle kimlik kontrolü her iki aşamada da yapılmalı, her iki aşamada da müşterinin ve kupon sağlayıcının iddia ettiği kişi olup olmadığı kontrol edilmelidir.

Bu sorunu çözmek için karşılıklı kimlik kontrolü (mutual authentication) yöntemi (örnek olarak Alshehri ve diğ., (2013), Chang ve Sun (2014) algoritmaları) veya karşılıklı kimlik kontrolüne ilave olarak müşterinin sahip olduğu fiziksel özellikleri de kontrol aşamasına ekleyen yöntemler de (müşterinin parmak izini kimlik kontrolü olarak kullanan algoritma (Zhu ve diğ., 2015)) kullanılabilir.

Biz burada karşılıklı kimlik kontrolü için basit ama etkili bir yöntem olan, gönderilen bilginin sadece gizli anahtara sahip olan kullanıcı tarafından açılabileceği, veriyi gönderenin de gönderdiği veriyi gizli anahtarı ile imzalamasıyla da alıcı tarafından kimliğinin kontrol edilebileceği bir yöntem olan, açık anahtarlı şifreleme sistemini kullandık.

Müşterinin bilgilerinin çalınması ve müşterinin almış olduğu kuponun geçersiz hale getirilmesi saldırılarını engellemek için hazırlanan algoritmanın düzenlenmiş hali Şekil 3.6'da sunulmuştur. İlk aşamada müşteri öncelikle kendi ID değerini (ID_m) ve rasgele üretmiş olduğu N_m değerini kupon sağlayıcıya gönderir (Eşitlik (3.17)). N_m değeri kupon sağlayıcının kimliğini kontrol etmek amacıyla müşteri tarafından kullanılacaktır. ID_m ve N_m değerlerini alan kupon sağlayıcı kendi kimliğini ispatlamak için N_m değerini geri göndermek zorundadır. Bu değeri geri göndermeden önce kendisi de rasgele bir sayı (N_f) üretir ve N_m ile birleştirir. N_f değeri de müşterinin kimliğini kontrol etmek için kupon sağlayıcı tarafından kullanılacaktır. Kupon sağlayıcı kendi kimliğini ispatlamak için müşteriden gelen N_m değerini kendi gizli anahtarı (KR_f) ile imzalar ($E(N_m \parallel N_f, KR_f)$) ve göndermiş olduğu verilerin sadece müşteri tarafından açılmasını sağlamak için de imzaladığı veriyi müşterinin açık anahtarı ile şifreler (Eşitlik (3.18) ($E(E(N_m \parallel N_f, KR_f), KU_m)$. Müşteri Eşitlik (3.18) ile gönderilen şifreli verileri aldıktan sonra önce kendi gizli anahtarını sonra da kupon sağlayıcının açık anahtarını kullanarak şifreyi çözer ve N_m' ve N_f değerlerini elde eder. Eğer gelen N_m' ile kendi göndermiş olduğu N_m aynı ise kupon sağlayıcının kimliği onaylanmış olur. Müşteri de istemiş olduğu m-kuponu alabilmek ve kimliğini kupon sağlayıcıya ispatlayabilmek için N_f ve PIN değerlerini imzalayıp kupon sağlayıcının açık anahtarı ile şifreler ve kupon sağlayıcıya gönderir (Eşitlik

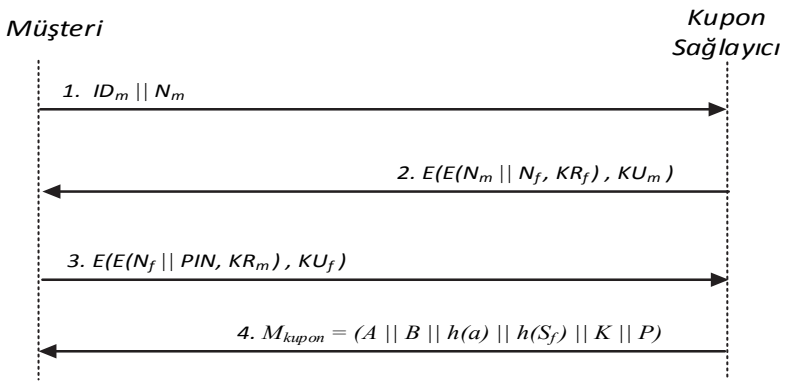
(3.19)). Kupon sağlayıcı gelen verilerin şifrelerini çözdükten sonra N_f' değeri ile kendi göndermiş olduğu N_f değerini karşılaştırır. Eğer ikisi de aynı ise müşterinin de kimliği onaylanmış olur ve kupon sağlayıcı müşterinin istemiş olduğu M_{kupon} bilgisini gönderir.

Yapılan bu düzenleme ile hem oltalama, kimlik bilgilerinin çalınması, yetkisiz kupon kullanma/üretme ve kuponun geçersiz kılınması saldırıları engellenmiş hem de kupon sağlayıcı ve müşterinin karşılıklı olarak kimlik kontrolü yapması sağlanmıştır. Düzenleme ile sisteme iki defa imzalama ve şifreleme işlemi eklenmiştir. Yapılan bu eklemeler ile her ne kadar müşterinin kaynaklarının daha fazla kullanıldığı düşünülse de, bu aşamalar olmadan sisteme yapılabilecek saldırılar düşünüldüğünde, müşterinin ve firmanın güvenliği açısından önemsiz kalmaktadır. Ayrıca, mevcut mobil cihazlar özellikleri bakımından bu ilave işlemleri kolaylıkla yapabilecek kapasitede olup güvenlik için göze alınması zorunlu olan bir maliyettir.

$$ID_m \,||\, N_m \tag{3.17}$$

$$E(E(N_m \,||\, N_f\,,\, KR_f), KU_m) \tag{3.18}$$

$$E(E(N_f \,||\, PIN\,,\, KR_m), KU_f) \tag{3.19}$$



Şekil 3.6. Kuponun oluşturulması aşamasındaki açıklığın giderilmesi

3.2.3.2. Gizli anahtarın elde edilmesi saldırısına çözüm önerisi

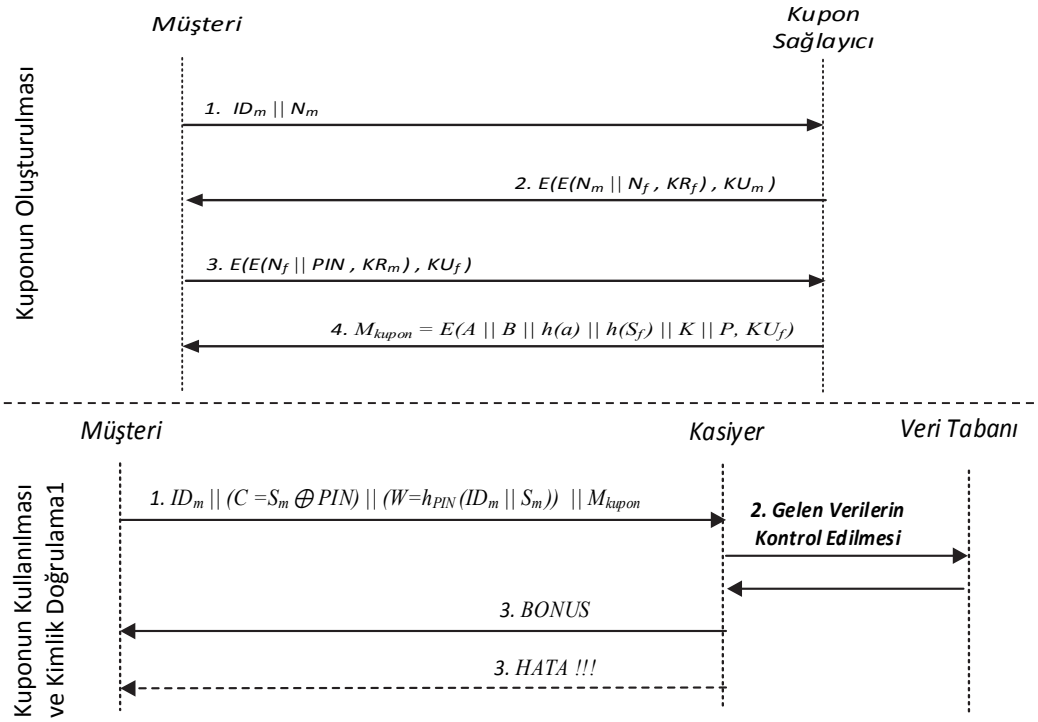
Algoritmada, kupon sağlayıcı tarafından müşteriye gönderilen m-kupon (M_{kupon}) sadece kasiyer tarafından kullanılmakta, müşteri üzerinde herhangi bir işlem yapmadan M_{kupon} değerini saklamaktadır. Bu nedenle gönderilen M_{kupon} bilgisinin

açık olarak gönderilmesinin bir avantajı bulunmamakta, tam aksine açık olarak gönderildiğinde sistem saldırıya açık hale gelmekte ve saldırganlar gizli anahtarı (x) elde edebilmektedir.

Gizli anahtarın elde edilmesi saldırısını önlemek için kupon oluşturulması aşamasında müşteriye gönderilen m-kupon verileri kupon sağlayıcının açık anahtarıyla şifrelenmelidir:

$$M_{kupon} = E\,(A \,||\, B \,||\, h(a) \,||\, h(S_f) \,||\, K \,||\, P,\, KU_f) \tag{3.20}$$

Güvenliği sağlamak için, Eşitlik (3.20) ile ekstra yapılan açık anahtarlı şifreleme yöntemi süreci olumsuz olarak etkilemeyecektir. Çünkü şifreleme işlemi (Şekil 3.7'de kuponun oluşturulması aşamasındaki ikinci adım) ve şifrenin çözülmesi işlemi (Şekil 3.7'de kuponun kullanılması ve kimlik doğrulama aşamasındaki ikinci adım) tamamıyla firma tarafından yapılacak olup firmanın sistemleri de bu ilave yükü kolaylıkla kaldırabilecek düzeydedir. Müşteri, M_{kupon} verisi üzerinde herhangi bir işlem yapmamaktadır. Müşterinin bilgilerinin çalınması, yetkisiz kupon kullanma/üretme ve kuponun geçersiz kılınması saldırılarının önlenmesi için yapılan çözüm de eklenerek hazırlanan algoritmanın son hali Şekil 3.7'de gösterilmiştir.



Şekil 3.7. Yeniden düzenlenen algoritma

3.2.4. Algoritmanın güvenlik analiz aracı Scyther ile analizi

3.2.4.1. Scyther analiz aracı

Scyther aracı tüm olası protokol/algoritma davranışlarının sonlu bir sunumunu yaparak protokolleri/algoritmaları karakterize edebilen güçlü bir güvenlik protokol/algoritma analiz aracıdır. Bu araç, atakların, olası protokol/algoritma davranışlarının ve protokollerin/algoritmaların doğruluğunun kontrol edilmesini ve hataların tespit edilmesini sağlar (Cremers, 2008).

Scyther aracı kullanılarak yapılan protokol/algoritma analizleri arasında ISO/IEC 11770 standardı (Cremers ve Horvat, 2014), Taha ve arkadaşları tarafından yapılan IEEE 802.16 güvenlik alt katmanının analizi (Taha ve diğ., 2009), Basin ve arkadaşları tarafından yapılan ISO/IEC 9798 varlık kimlik doğrulama standardı (Basin ve diğ., 2013), Cas Cremer tarafından yapılan internet anahtar değişim protokollerinin (IKEv1 ve IKEv2) analizi (Cremers, 2011) sayılabilir. Yapılan bu analizler içerisine en dikkat çekici olan IKEv1 ve IKEv2 internet anahtar değişim protokollerinin güvenlik analizidir. IKEv2 çok kullanılan bir protokol olup protokolün güvenlik analizinin nasıl yapıldığı Cas Cramer tarafından gösterilmiştir (Cremers, 2011). Kodlamaların nasıl yapılacağı ile ilgili detaylar Scyther Kullanım Kılavuzunda (Cremers, 2014) gösterilmektedir.

Scyther aracı kullanılarak yapılan onlarca analiz bulunmaktadır. Bahse konu analizlere (Selected protocol models for our analysis tools, URL-1) ve diğer incelemelere ulaşmak için web sayfaları (Cas Cremers Publications, URL-2) ziyaret edilebilir.

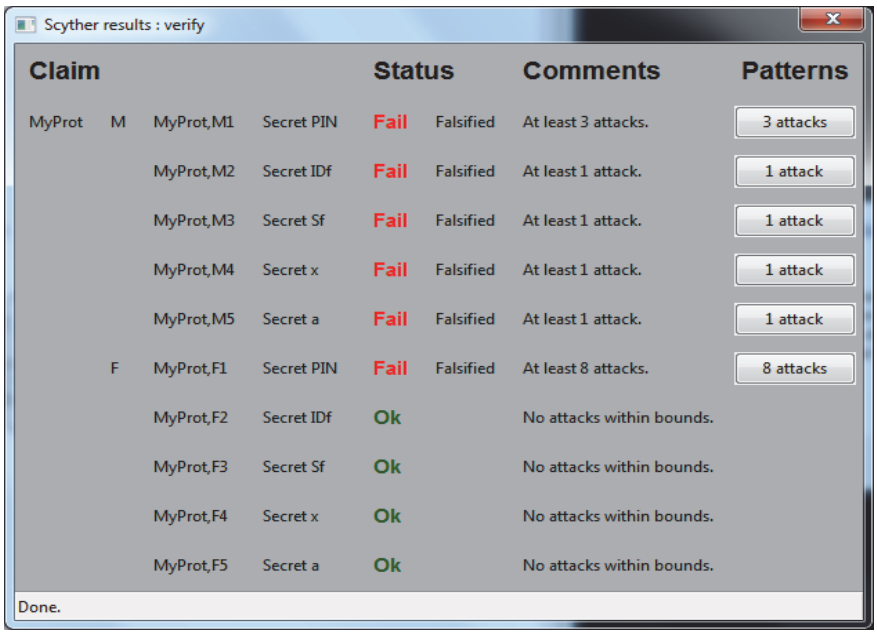
3.2.4.2. Scyther aracı ile analiz

Hsiang algoritmasını Scyther kılavuzuna (Cremers, 2014) göre kodlarken algoritmada yer alan katılımcılar (müşteri (M), kupon sağlayıcı ve kasiyer (F)) "role" olarak tanımlandı (role M, role F). Burada kupon sağlayıcı ve kasiyer aynı firmanın parçası oldukları için tek bir varlık olarak (F) ele alındı ve "role F" olarak kodlandı. Bir algoritmada herhangi bir sayıda "role" olabilir ve algoritmada yer alan varlıkların yapacağı işlemler bu roller aracılığı ile gösterilir. Roller send, receive ve claim

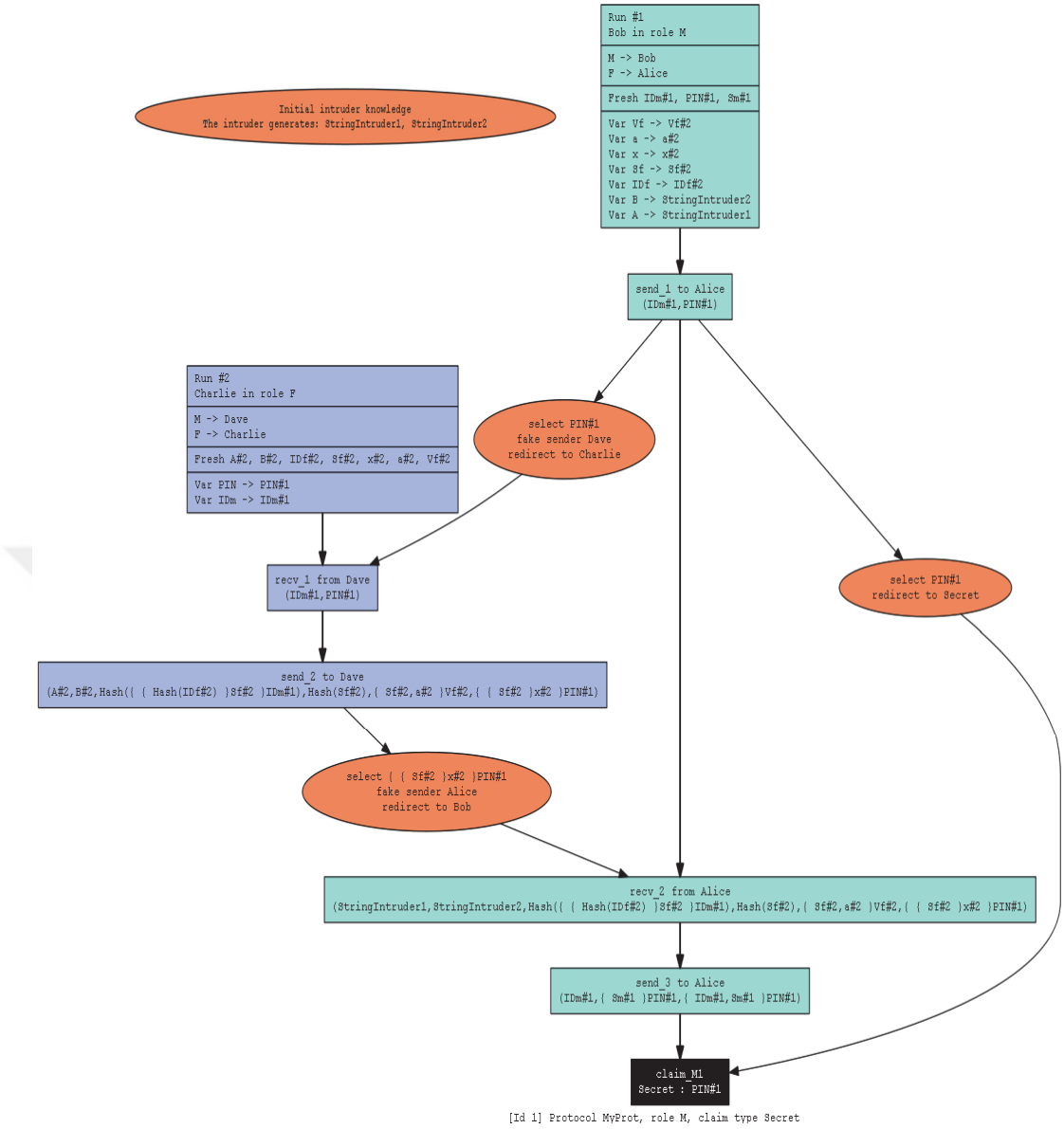
parametrelerinden oluşmaktadır. Burada karşı tarafa gönderilecek veriler send parametresi, gelen veriler receive parametresi ve saldırganlardan korunması gereken veriler claim parametresi olarak gösterilir. Analize başlamadan önce bilinmesi gereken önemli bir husus da Scyther'in, algoritmada kullanılan simetrik/asimetrik şifreleme sistemlerinin, özet (hash) fonksiyonlarının güvenlik açığı barındırmadığını ve bu fonksiyonların kriptografik olarak güvenilir olduğunu kabul etmesidir.

Burada yapmış olduğumuz çalışmada, Hsiang tarafından geliştirilen algoritmanın analizi için Scyther v1.1.3 Windows sürümünü kullandık. Algoritmadaki rolleri ve değişkenleri tanımladıktan sonra saldırgandan korunması gereken verileri belirledik ve korunması gereken verileri claim parametresi ile gösterdik. Algoritmanın, bu değerlerin güvenliğini/gizliliğini sağlaması gerekmektedir. Yapılan kodlama (Hsiang_algoritmasi.spdl) Ek-B'de verilmiştir.

Analiz sonucunda Hsiang'ın algoritmasının belirtildiği kadar güçlü olmadığı, algoritmada açık olduğu, korunması gereken verilerin gizliliğini/güvenliğini sağlayamadığı ve bu açık kullanılarak saldırılar yapılabileceği Scyther aracı tarafından da teyit edilmiştir (Şekil 3.8). Analiz sonucu bizim oyun kuramı ile yapmış olduğumuz analiz ile de örtüşmekte olup Scyther aracı tarafından tespit edilen tüm saldırıların, bizim de daha önce tespit ettiğimiz gibi, kuponun oluşturulması aşamasındaki açıktan kaynaklandığı görülmüştür.



Şekil 3.8. Algoritmanın Scyther aracı ile yapılan analizinin sonucu



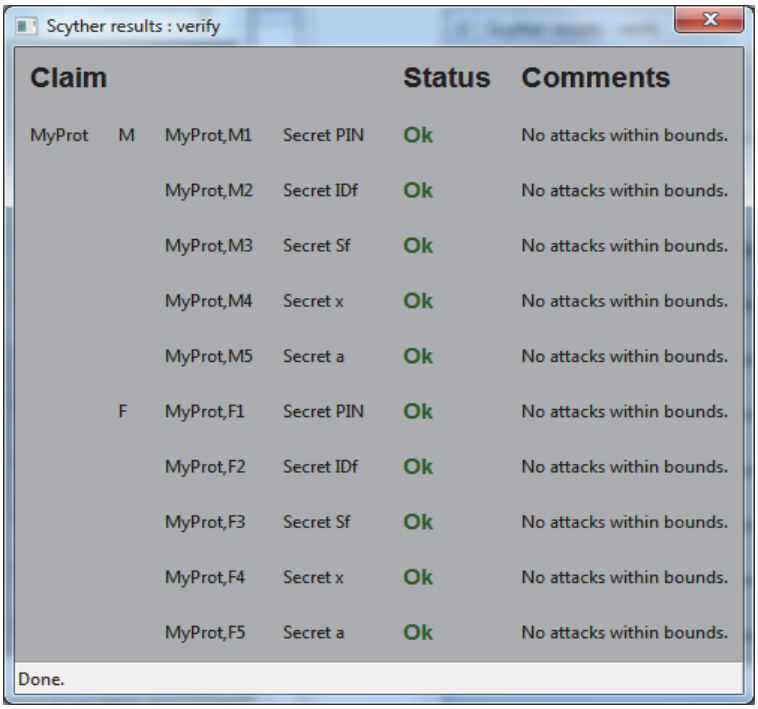
Şekil 3.9. Scyther aracı ile tespit edilen örnek bir saldırı

Şekil 3.8'de verilen analiz sonucunda da görüleceği üzere algoritmaya yönelik toplamda 15 adet saldırı tespit edilmiş olup araç tarafından tespit edilen saldırılardan birisi Şekil 3.9'de gösterilmiştir. Yapılan bu saldırıda algoritma iki kez işletilmiştir. Birincisinde müşteri olarak Bob, firma olarak Alice, ikincisinde müşteri olarak Dave, firma olarak Charlie yer almıştır. Burada saldırgan Bob ile Alice arasındaki iletişimi dinlemekte, elde ettiği IDM#1 ve PIN#1 verilerini başka bir müşteri gibi davranarak ikinci iletişimdeki Dave adına Charlie'ye göndermektedir. Charlie gelen bu değerleri alarak send_2 değerini yani M_{kupon} verisini hesaplayıp saldırgana geri göndermektedir. Böylece saldırgan hem M_{kupon} bilgisini elde etmekte, hem de Bob'un IDM#1 ve PIN#1 verilerini kullanarak sistemi manipüle edebilmektedir.

Daha sonra, hem bizim hem de Scyther tarafından tespit edilen açıkları gidermek için Şekil 3.7'de gösterilen önermiş olduğumuz algoritmanın, gerçekten bizim iddia ettiğimiz gibi gerekli güvenlik kriterlerini sağlayıp sağlamadığını kontrol etmek amacıyla, önerdiğimiz algoritmayı Scyther kılavuzuna (Cremers, 2014) göre kodladık. Yapılan kodlama (Hsiang_algoritmasi_onerilen_hali.spdl) Ek-C'de verilmiştir. Yapılan analiz sonucunda önerilen yapının gerekli güvenliği sağladığı ve herhangi bir saldırının yapılamadığı tespit edilmiştir. Algoritmaya yönelik olarak yapılabilen saldırılar Tablo 3.2'de ve önerilen algoritmanın Scyther aracı ile yapılan analiz sonucu Şekil 3.10'da verilmiştir.

Tablo 3.2. Algoritmaya yapılabilen saldırılar

Saldırının Adı	**Hsiang**	**Önerilen Algoritma**
Yetkisiz kupon kullanma saldırısı	EVET	HAYIR
Yetkisiz kupon kopyalama/çoğaltma	HAYIR	HAYIR
Yetkisiz kupon üretme saldırısı	EVET	HAYIR
Veri değiştirme saldırısı	EVET	HAYIR
Kuponun çoklu kullanılması saldırısı	HAYIR	HAYIR
Yeniden gönderme saldırısı	HAYIR	HAYIR
Gizli anahtarın elde edilmesi	EVET	HAYIR



Şekil 3.10. Önerilen algoritmanın Scyther aracı ile yapılan analizinin sonucu

4. ONAY KODLU M-KUPON ALGORİTMASI (MCWCC)

NFC özellikli mobil cihazların giderek yaygınlaşacağı ve günlük yaşantının bir parçası olacağı düşünüldüğünde, kullanıcıların hayatlarını kolaylaştırırken güvenlik endişelerini ortadan kaldıracak sistem/algoritmalara olan ihtiyaç da giderek artmaktadır. Bu kapsamda, Hsueh ve Chen algoritması ile Hsiang algoritmasının güvenlik analizlerinden elde ettiğimiz tecrübeler doğrultusunda, hem kullanımı kolay olan, hem tüm kullanıcılarının güvenliğini garanti altına alan, hem de güvenlik analizleri Scyther gibi otomatik güvenlik algoritması doğrulama aracı ile yapılmış, güvenilir ve uygulanabilir yeni bir m-kupon algoritması geliştirdik.

4.1. Algoritmanın Genel Yapısı

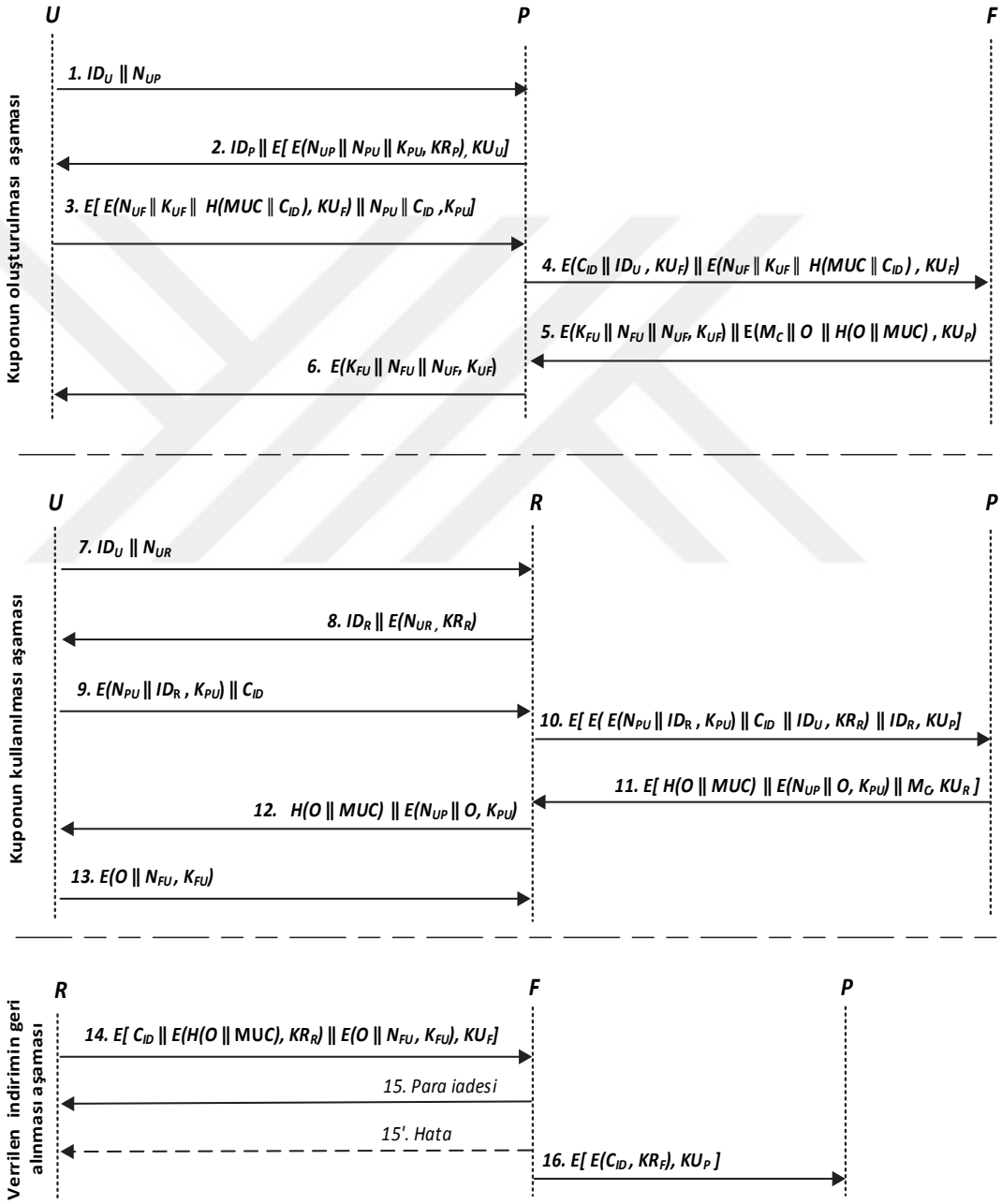
Sunmuş olduğumuz m-kupon algoritması MCWCC (M-Coupon protocol With Confirmation Code) Şekil 2.2'de verilen genel m-kupon modeliyle aynı yapıya sahiptir. Bu yapıda algoritmada dört katılımcı yer almaktadır: Üretici firma (Manifacturer (F), kupon sağlayıcı (coupon provider (P)), kullanıcı veya müşteri (user (U)) ve satıcı/kasiyer (retailer (R)). İlk önce m-kuponu kullanabilmek için müşteri bir m-kupon almalıdır (kuponun oluşturulması aşaması), daha sonra verilen indirimi alabilmek için kuponu kullanmalıdır (kuponun kullanılması aşaması), en son olarak ta indirimi vererek gelirinin bir kısmını kaybeden kasiyer vermiş olduğu indirimi üretici firmadan gelir almak ve kuponun tekrar kullanımını önlemek için kullanım bilgilerini üretici firmaya gönderir (verilen indirimin geri alınması aşaması). Algoritmada kullanılan sembollerin anlamları simgeler ve kısaltmalar dizini altında, MCWCC algoritması Şekil 4.1'de verilmiştir.

4.1.1. Kuponun oluşturulması aşaması

Kuponun elde edilmesi aşamasında müşteri bir m-kupon sağlayıcıya (kupon sağlayıcının web sayfası, NFC poster vb.) gider ve bir m-kupon talep eder. Şekil 4.1'de de görüleceği üzere kuponun oluşturulması aşaması altı adımdan oluşmaktadır. Bu adımlar:

Adım 1: Müşteri (U), m-kuponu elde etmek için kimlik bilgisini (ID_U) ve üretmiş olduğu rasgele değeri (N_{UP}) kupon sağlayıcıya (P) gönderir Eşitlik (4.1). N_{UP} değeri algoritmanın ileriki aşamalarında U tarafından P'nin kimliğini kontrol etmek için kullanılacak.

$$ID_U \parallel N_{UP} \tag{4.1}$$



Şekil 4.1. Onay kodlu m-kupon algoritması (MCWCC)

Adım 2: P sonraki adımlarda kullanılacak N_{PU} ve K_{PU} değerlerini hesaplar. N_{PU} değeri rasgele bir değer olup U'nun kimliğini kontrol etmek amacıyla kullanılacak. K_{PU} değeri bir sonraki adımda U ve P arasında kurulacak olan iletişimde gönderilecek verilerin şifrelenmesinde kullanılacak olan simetrik anahtardır. Bu iki değer sayesinde (N_{PU} ve K_{PU}) P simetrik şifreleme sistemi kullanarak U'nun kimliğini kontrol edebilecektir. P kimliğini U'ya ispatlamak için N_{UP} değerini göndereceği değerlere ekler ve kendi gizli anahtarı ile şifreler ($E(N_{UP} \| N_{PU} \| K_{PU}, KR_P)$). Göndermiş olduğu mesajın doğru kişi tarafından alındığından emin olmak ve şifrelemiş olduğu verilerin sadece U tarafından açılabileceğinden emin olmak için mesajı U'nun açık anahtarı ile şifreler. P ayrıca U'ya kendi kimlik bilgisini de (ID_P) ekleyip gönderir Eşitlik (4.2).

$$ID_P \| E(\ E(N_{UP} \| N_{PU} \| K_{PU}, KR_P),\ KU_U) \tag{4.2}$$

Adım 3: ID_P değerini elde ettikten sonra U gelen mesajın şifresini çözerek N_{UP}, N_{PU}, K_{PU} değerlerini elde eder. N_{UP} değeri ilk adımda U tarafından P'ye gönderilmişti. Gelen mesajdan elde etmiş olduğu N_{UP}' değer ile kendi göndermiş olduğu N_{UP} değeri karşılaştırır. Eğer iki değer de aynı ise U, P'nin kimliğini kontrol etmiş ve onaylamış olur.

U m-kuponu elde etmeden önce birkaç değeri daha hesaplamalıdır. İlk önce N_{UF}, K_{UF}, ψ değerlerini hesaplar. Bu değerler algoritmanın ilerleyen adımlarında F ile yapılacak olan iletişimde kullanılacaktır. N_{UF} değeri kontrol amacıyla kullanılacak değer, K_{UF} değeri U ile F arasında kurulacak olan iletişimde kullanılacak olan simetrik anahtar ve ψ değeri ($\psi = H(MUC \| C_{ID})$) F tarafından U'nun kimliğini kontrol etmek amacıyla kullanılacak olan değerdir. ψ değeri sayesinde U'nun kimlik kontrolü açık anahtarlı şifreleme sistemi kullanılmadan yapılacaktır. MUC değeri Mobil device Unique Code (MUC) yalnızca F ve U tarafından bilinen, U'nun sadık müşteri programına katılımında oluşturulan eşsiz bir değerdir. Bu değer U'nun mobil cihazını tanımlamaktadır. C_{ID} m-kuponun seri numarasıdır. Özet değerine C_{ID}'nin eklenmesi sayesinde ψ değeri her seferinde değişecektir. U daha sonra N_{UF}, K_{UF}, ψ değerlerini F'nin açık anahtarı ile şifreleyerek α değerini ($\alpha = E(N_{UF} \| K_{UF} \| \psi, KU_F)$) elde eder.

U kimliğini P'ye ispatlayabilmek için N_{PU} değerini mesaja ekler. Ayrıca mesaja C_{ID} değerini de ekler ve ikinci adımda P tarafından kendisine gönderilen simetrik anahtarı (K_{PU}) kullanarak şifreler ($E(\alpha \parallel N_{PU} \parallel C_{ID}, K_{PU})$).

P gelen mesajın ($E(\alpha \parallel N_{PU} \parallel C_{ID}, K_{PU})$) şifresini kendi göndermiş olduğu K_{PU} değerini kullanarak çözer ve α, C_{ID} ve N_{PU}' değerlerini elde eder. Elde etmiş olduğu N_{PU}' ile kendi göndermiş olduğu N_{PU} değerlerini karşılaştırır. Eğer iki değer aynı ise U'nun kimliği kontrol edilmiş ve onaylanmış olur. α değeri sadece daha sonra kullanılmak üzere saklanır, üzerinde işlem yapılamaz, çünkü bu değer F'nin açık anahtarı ile şifrelenmiştir Eşitlik (4.3).

$$E(E(N_{UF} \parallel K_{UF} \parallel H(MUC \parallel C_{ID}), KU_F \parallel N_{PU} \parallel C_{ID}, K_{PU}) \quad (4.3)$$

Adım 4: Bu adıma kadar P tarafından U'nun kimliği kontrol edildi ve U'nun istemiş olduğu m-kuponun seri numarası elde edildi. Bu adımda P, C_{ID} ve ID_U değerlerini F'nin açık anahtarını kullanarak şifreler, daha sonra α değeri ile birlikte F'ye gönderir Eşitlik (4.4).

$$E(C_{ID} \parallel ID_U, KU_F) \parallel E(N_{UF} \parallel K_{UF} \parallel H(MUC \parallel C_{ID}), KU_F) \quad (4.4)$$

P, U'nun ID_U değerini özellikle F'ye gönderir. Böylelikle F, U'nun kimliğini kontrol edebilir, P'nin bir saldırgan olmadığını anlayabilir ve m-kuponu talep eden gerçek bir müşterinin var olduğundan emin olabilir. F bu kontrolü ψ değeri üzerinden yapar. F, P'den gelen mesajın şifresini çözer ve elde ettiği ID_U değerini kullanarak veri tabanından U'nun MUC değerini bulur. Daha sonra MUC ve C_{ID} değerlerini kullanarak özet değerini ($H(MUC \parallel C_{ID})$) hesaplar. Eğer bu özet değeri ψ değeri ile aynı ise U'nun kimliği kontrol edilmiş olur. N_{UF} değeri U tarafından F'nin kimliğinin kontrol edilmesi amacıyla kullanılacaktır. K_{UF} değeri F tarafından U'ya gönderilecek olan verilerin şifrelenmesi amacıyla kullanılacak olan simetrik anahtardır.

Adım 5: Kontrol süreci tamamlandıktan sonra F, K_{FU} ve N_{FU} değerlerini hesaplar. N_{FU} değeri F tarafından U'nun kimliğinin kontrol edilmesi amacıyla kullanılacaktır. K_{FU} değeri, U tarafından m-kuponun kullanımından sonra F'ye gönderilecek olan onay kodunun (O) şifrelenmesinde kullanılacak olan, simetrik anahtardır. F, Ω değerini hesaplar ($\Omega = E(K_{FU} \parallel N_{FU} \parallel N_{UF}, K_{UF})$).

F, gönderilen m-kuponun asıl talep eden müşteri tarafından kullanılıp kullanılmadığını kontrol etmek için kullanacağı onay kodunu (O) belirler. Bu kod U'ya P üzerinden gönderilecektir. Burada F sadece O değerini göndermez, bununla birlikte O ve MUC değerlerinin özet değerini (H (O || MUC)) hesaplayarak U'ya gönderir. U, O değerini kullanarak özet değerini (H (O || MUC)) yeniden hesaplar. Eğer iki özet değeri de aynı ise onay kodunun hatasız/sorunsuz olarak ulaştığı anlaşılacaktır. Aksi durumda ise onay kodunun yolda bozulduğu veya üzerinde oynandığı sonucuna ulaşılacaktır. F daha sonra indirim bilgisini (M_C) mesaja ekleyerek P'nin açık anahtarı ile şifreler ve Ω değeri ile birlikte P'ye gönderir Eşitlik (4.5).

$$E(K_{FU} \,||\, N_{FU} \,||\, N_{UF}, K_{UF}) \,||\, E(M_C \,||\, O \,||\, H(O \,||\, MUC), KU_P). \quad (4.5)$$

Adım 6: P gelen mesajın şifresini çözer, kendisinde kalacak olan verileri Ω değerinden ($\Omega = E(K_{FU} \,||\, N_{FU} \,||\, N_{UF}, K_{UF})$) ayırır ve Ω değerini U'ya transfer eder Eşitlik (4.6).

$$E(K_{FU} \,||\, N_{FU} \,||\, N_{UF}, K_{UF}) \quad (4.6)$$

U gelen mesajı kontrol etmek için mesajın şifresini kendi göndermiş olduğu K_{UF} simetrik anahtarını kullanarak çözer ve N_{UF}' değerini elde eder. Eğer gelen N_{UF}' değeri ile kendi göndermiş olduğu N_{UF} değerleri aynı ise mesajı gönderenin gerçekten F olduğunu anlar ve K_{FU} ve N_{FU} değerlerini sonraki adımlarda kullanmak üzere saklar.

4.1.2. Kuponun kullanılması aşaması

M-kuponu kullanmak için U telefonunu R'nin cihazına temas ettirmelidir. Kuponun kullanılması aşaması yedi adımdan oluşmaktadır (Şekil 4.1, 7. adımdan 13. adıma kadar).

Adım 7: U kendi kimlik bilgisini (ID_U) ve rasgele sayıyı (N_{UR}) R'ye gönderir Eşitlik (4.7). N_{UR} değeri U tarafından R'nin kimlik bilgilerinin kontrol edilmesi amacıyla kullanılacaktır.

$$ID_U \,||\, N_{UR} \quad (4.7)$$

Adım 8: R gelen mesaj içinden N_{UR} değerini alır ve kendi gizli anahtarı ile şifreler ($E(N_{UR}, KR_R)$), bu değere kendi kimlik bilgisini (ID_R) ekler ve U'ya gönderir Eşitlik (4.8).

$$ID_R \,||\, E(N_{UR}, KR_R) \tag{4.8}$$

U gelen mesajın şifresini R'nin açık anahtarını kullanarak çözer ve N_{UR}' değerini elde eder. Elde ettiği N_{UR}' değeri ile kendi göndermiş olduğu N_{UR} değerini karşılaştırır. Böylelikle U kasiyerin kimliğini kontrol etmiş olacaktır.

Adım 9: Bu adıma kadar kasiyer U'nun kimlik bilgilerini kontrol etmedi. Bu kontrol işlemi P tarafından yapılacaktır. U kimliğini ispat etmek için kendisine kuponun oluşturulması aşamasında P tarafından gönderilen N_{PU} ve K_{PU} değerlerini kullanır. Bunun için N_{PU} değerine ID_R bilgisini de ekleyerek K_{PU} ile şifreler. Daha sonra λ değerini ($\lambda = E(N_{PU} \,||\, ID_R, K_{PU}) \,||\, C_{ID}$) hesaplamak için C_{ID} değerini ekler ve sonucu R'ye gönderir Eşitlik (4.9).

$$E(N_{PU} \,||\, ID_R, K_{PU}) \,||\, C_{ID} \tag{4.9}$$

Adım 10: Kasiyer herhangi bir işlem yapmadan ID_U verisini gelen mesaj üzerine ekler ve kendi gizli anahtarı ile şifreler. Daha sonra bu değere kendi ID_R değerini ekleyerek tamamını P'nin açık anahtarı ile şifreler ve P'ye gönderir Eşitlik (4.10).

$$E(\, E(E(N_{PU} \,||\, ID_R, K_{PU}) \,||\, C_{ID} \,||\, ID_U, KR_R) \,||\, ID_R, KU_P) \tag{4.10}$$

P'ye gönderilen mesajda ID_R bilgisi iki kez yer almaktadır. Birisi U tarafından eklenen birisi de R tarafından eklenen değerdir. Bu iki değer sayesinde P hem R ile iletişim kuran U'nun hem de U ile iletişim kuran R'nin aynı kişiler olup olmadığını kontrol etmektedir. Ayrıca U'nun kimliği ID_U değeri üzerinden kontrol edilmektedir.

Bu kontrolü yapabilmek için P veri tabanından ID_U ve C_{ID} değerlerini kullanarak U'nun verilerine ulaşır. Buradan kendi göndermiş olduğu K_{PU} ve N_{PU} değerlerini bulur. P gelen mesajın ($\lambda = E(N_{PU} \,||\, ID_R, K_{PU}) \,||\, C_{ID}$) şifresini K_{PU} anahtarını kullanarak çözer. Daha sonra elde edilen N_{PU}' değeri ile kendi göndermiş olduğu N_{PU} değerlerini karşılaştırır. Eğer iki değer de aynı ise U'nun kimliği kontrol edilmiş ve onaylanmış olur. Sonrasında ID_R' değerini kullanarak kasiyerin kimliğini kontrol

eder. Şifreyi çözerek elde etmiş olduğu ID_R' değeri ile U'nun göndermiş olduğu ID_R değerleri aynı ise R'nin de kimliği kontrol edilmiş olur.

Adım 11: Yapılan kontroller ile hem U'nun hem de R'nin kimlikleri kontrol edilmiş oldu. Artık P hem indirimi hem de onay kodunu (O) R'ye gönderebilir. Bunun için P, N_{UP} ve O değerlerini K_{PU} simetrik anahtarı ile şifreler. ϕ değerini hesaplamak için P, F tarafından gönderilen özet değerini $E(N_{UP} \| O, K_{PU})$ değerine ekler ($\phi = H(O \| MUC) \| E(N_{UP} \| O, K_{PU})$). Daha sonra hesaplamış olduğu ϕ değerine indirim oranını gösteren M_C değerini de ekleyerek R'nin açık anahtarı ile şifreler ($E(\phi \| M_C, KU_R)$) Eşitlik (4.11).

$$E(H(O \| MUC) \| E(N_{UP} \| O, K_{PU}) \| M_C, KU_R) \quad (4.11)$$

Adım 12: R kendisine P tarafından gönderilen mesajı aldıktan sonra kendi gizli anahtarı ile şifreyi çözer. İndirim oranını gösteren M_C değerini ϕ değerinden ayırır ve ϕ değerini U'ya gönderir Eşitlik (4.12).

$$H(O \| MUC) \| E(N_{UP} \| O, K_{PU}) \quad (4.12)$$

U gelen mesajın ($E(N_{UP} \| O, K_{PU})$) şifresini kendi göndermiş olduğu K_{PU} simetrik anahtarını kullanarak çözer ve N_{UP}' ile O' değerlerini elde eder. Eğer elde etmiş olduğu N_{UP}' değeri ile kendisinde bulunan N_{UP} değerleri aynı ise P'nin kimliği kontrol edilmiş olur. U daha sonra elde etmiş olduğu O' değerini kontrol etmek için MUC değeri ile birlikte özet değerini hesaplar $H(O' \| MUC)$. Eğer gelen özet değeri ile hesaplanan özet değerleri aynı ise O değerinin yolda değişmediği anlaşılır.

Adım 13: U yapmış olduğu kontroller ile P ve R'nin kimliğini ve O değerinin yolda değişmediğini onaylamış oldu. Bu noktadan sonra artık indirimi aldığını F'ye bildirmesi gerekmektedir. Bu amaçla U, N_{FU} ve O değerlerini K_{FU} simetrik anahtarı ile şifreleyerek R'ye gönderir Eşitlik (4.13). Bu mesaj R tarafından, indirimi U'ya verdiğini ispatlamak üzere, verilen indirimin geri alınması aşamasına kadar saklanacaktır.

$$E(O \| N_{FU}, K_{FU}) \quad (4.13)$$

4.1.3. Verilen indirimin geri alınması aşaması

R vermiş olduğu indirim nedeniyle gelirinin bir kısmını kaybetmiş oldu. Bunu geri alabilmek için:

Adım 14: R, m-kupon seri numarasına (C_{ID}) P'den gelen özet değerini (H(O || MUC)) ekler ve kendi gizli anahtarı ile şifreler. Bu değeri de U'dan gelen E(O || N_{FU}, K_{FU}) değerine ekleyerek F'nin açık anahtarıyla şifreler ve F'ye gönderir Eşitlik (4.14).

$$E(C_{ID} \,||\, E(H(O \,||\, MUC), KR_R) \,||\, E(O \,||\, N_{FU}, K_{FU}), KU_F) \quad (4.14)$$

Adım 15: F, gelen mesajın şifresini çözer ve özet değerini (H(O || MUC)) elde eder. Gelen mesajdan elde ettiği C_{ID} değerini kullanarak veri tabanından U'nun bilgilerine erişir. Kendi göndermiş olduğu K_{FU} simetrik anahtarını kullanarak U tarafından şifrelenmiş olan verilerin şifresini çözerek O′ ve N_{FU}′ değerlerini elde eder. Eğer elde ettiği N_{FU}′ değeri ile kendi göndermiş olduğu N_{FU} değerleri aynı ise O′ ve O değerlerini karşılaştırır. Eğer bu değerler de aynı ise F, R'nin U'ya vermiş olduğu indirimi R'ye iade eder Eşitlik (4.15).

ONAY veya RET (4.15)

Eğer O ve O′ değerleri aynı değil ise F kendi veri tabanında bulunan özet değeri (H(O || MUC)) ile R tarafından şifrelenerek gönderilen özet değerini (E(H(O || MUC), KR_R)) karşılaştırır. Eğer bu iki değer farklı ise meydana gelen bozulmanın/hatanın P ile R arasında yapılan iletişimde ortaya çıktığı anlaşılacaktır. Yok, eğer bu iki değer aynı ise bozulma/hata R ile U arasında yapılan iletişimde ortaya çıktığı anlaşılacaktır. Algoritmaya eklenen bu özet değeri, hatanın hangi iletişimden kaynaklandığının tespit edilmesine olanak sağlamaktadır.

Adım 16: Son adım olarak, kuponun tekrar kullanımını önlemek için F, m-kuponun kullanılmış olduğunu P'ye bildirir Eşitlik (4.16).

$$E(E(C_{ID} , KR_F), KU_P) \quad (4.16)$$

4.2. MCWCC'nin Güvenlik Analizi

Bir algoritmanın saldırılara karşı dayanıklı olduğunu iddia edebilmek için algoritmanın güvenlik analizinin yapılması gerekmektedir. Yapılacak olan güvenlik analizi gizlilik, kimlik kontrolü, veri bütünlüğü, doğrulanabilirlik ve kuponun çoklu kullanımını içerir. M-kuponun güvenlik analizi hem satıcı hem de müşterinin güvenliği için zorunludur. Çünkü satıcılar/firmalar özel müşterileri için özel indirimler sunmak ve bu indirimlerin sadece indiriminin verildiği müşteriler tarafından kullanıldığından emin olmak isterler. Ayrıca herhangi bir saldırganın sistemi manipüle edemeyeceğinden ve gereksiz gelir kaybına uğramayacaklarından emin olmak isterler. Müşteriler ise istemiş oldukları veya kendilerine sunulan indirimi sorunsuz bir şekilde kullanmak isterler.

NFC teknik dokümanına (GSM Association, 2007) göre bir m-kupon algoritması ortadaki adam, gizlice dinleme, yeniden gönderme, veri düzenleme, yetkisiz kupon çoğaltma/üretme, kuponun çoklu kullanımları saldırılarına karşı dayanıklı olması gerekmektedir (Park ve Lee, 2013). Bazı saldırılar şifreli mesajların çözülmesine bile gerek olmadan, iletişime müdahale edilerek veya mesajların tekrar gönderilmesi ile de yapılabilmektedir.

Alshehri ve Briffa tarafından yapılan çalışmada (Alshehri ve diğ., 2013), Dominikus ve Aigner tarafından geliştirilen algoritmanın (Dominikus ve Aigner, 2007) güvenlik analizi Communicating Sequential Processes (CSP) (Hoare, 1985) ve model denetleyicisi Failures Divergence Refinement (FDR) (Ryan ve diğ., 2001) kullanılarak yapılmıştır. Yapmış oldukları analiz ile algoritmada bazı açıkların olduğunu ve bu açıkları kullanarak saldırıların yapılabileceğini tespit etmişlerdir.

Ancak burada göz önünde bulundurulması gereken önemli bir nokta bulunmaktadır; Dominikus ve Aigner tarafından geliştirilen algoritmanın (Dominikus ve Aigner, 2007) güvenlik analizi geliştiricileri tarafından değil başka araştırmacılar tarafından yapılmıştır. Eğer daha en başında önerilen algoritmanın güvenlik analizi geliştiricileri tarafından yapılmış olsaydı bu açıklar hiç olmayacaktı. Bu nedenle bu çalışmada geliştirmiş olduğumuz algoritmanın, iddia ettiğimiz gibi güvenli olup olmadığını anlamak ve göstermek için, güvenlik algoritmalarının doğrulanması amacıyla kullanılan Scyther analiz aracını (Cremers, 2008) kullanarak yaptık.

4.2.1. MCWCC'nin çok bilinen saldırılara karşı güvenlik analizi

Bu kısımda MCWCC'yi Scyter aracı ile analiz etmeden önce biz kendimiz çok bilinen saldırılara karşı analiz ettik.

4.2.1.1. Kimliğine bürünme saldırısına karşı dayanıklılık

Kimliğine bürünme saldırısını önlemek için hem açık anahtarlı şifreleme sistemi hem de kontrol amacıyla kullanılan rasgele sayılar (nonce) kullanılmıştır. Açık anahtarlı şifreleme sistemi ile yapılan şifreleme, sadece gizli anahtara sahip olan kullanıcı tarafından çözülebilir. Ayrıca rasgele sayılar sayesinde de kullanıcılar birbirlerinin kimliklerini kontrol edebilmektedirler. Örnek olarak; N_{UF}' değeri müşteri (U) tarafından üretici firmaya (F) algoritmanın üçüncü adımında gönderilmektedir (Şekil 4.1, adım 3). U bu değeri göndermeden önce F'nin açık anahtarı ile şifrelemekte, N_{UF} değerinin sadece F tarafından açılabileceğinden emin olmaktadır ($E(N_{UF} \parallel K_{UF} \parallel H(MUC \parallel C_{ID}) , KU_F)$). Böylelikle N_{UF} değeri üzerinden müşteri üreticinin firmanın kimliğini kontrol edebilmektedir. Bunun için algoritmanın altıncı adımında üretici tarafından gönderilen mesajın içerisinde (Şekil 4.1, adım 6) bu değere bakar, gelen N_{UF}' değeri ile kendi göndermiş olduğu N_{UF} değerini karşılaştırır. Eğer her iki değer de aynı ise müşteri doğru kullanıcı ile iletişim kurduğunu anlamaktadır.

4.2.1.2. Ortadaki adam saldırısına karşı dayanıklılık

Saldırgan tüm trafiği kontrol edebiliyor bile olsa, saldırgan hiçbir kullanıcının gizli anahtarını veya verileri şifrelemek için kullanılan simetrik anahtarları bilmemektedir. Saldırgan, kullanıcılardan birisinin gizli anahtarını bilmeden verileri şifrelemek için kullanılan simetrik anahtarı elde edemez, çünkü bu simetrik anahtarlar alıcıya alıcının açık anahtarıyla şifrelenerek gönderilmektedir. Ayrıca gelen mesajlar rasgele sayılar (N_{UF} gibi) üzerinden de kontrol edilmektedir. Eğer gönderilen rasgele sayı ile gelen rasgele sayılar aynı değil ise iletişim sonlandırılacaktır.

Yine ortadaki adam saldırısını önlemek için algoritmanın on üçüncü adımına başka bir kontrol değeri olan onay kodu (O) eklendi (Şekil 4.1, adım 13). Bu adımla müşteri onay kodunu, sunulan indirimi aldığını göstermek için, üreticiye gönderir.

Onay kodu üzerinden yapılan kontrollerin nasıl yapıldığı algoritmanın beşinci, on ikinci ve on üçüncü adımlarında detaylı olarak anlatılmıştır.

Ortadaki adam saldırısını önlemek için yapılan düzenlemelerden birisi de ID_U ve ID_R değerlerinin P'ye gönderilmesidir. Hem U hem de P kendi kimliklerini P'ye ispatlamak için kimlik bilgilerini gönderirler. Dokuzuncu adımda U, iletişim kurduğu kasiyerin ID_R bilgisini P'ye göndereceği mesajın içerisine ekler ($\lambda = E(N_{PU} \parallel ID_R, K_{PU}) \parallel C_{ID}$). Kimliğini P'ye ispatlamak isteyen R de onuncu adımda kendi kimlik bilgisi ID_R ile birlikte m-kuponu gönderen müşterinin ID_U değerini de P'ye gönderir ($E(E(\lambda \parallel ID_U , KR_R) \parallel ID_R , KU_P)$). Gelen mesajı alan P şifreleri çözdükten sonra N_{PU}, ID_U ve ID_R değerlerini kontrol eder. R'nin göndermiş olduğu ID_U ve C_{ID} bilgilerini kullanarak P veri tabanından simetrik anahtarı K_{PU} bulur. Bu anahtarı kullanarak müşteri tarafından gönderilen verinin ($E(N_{PU} \parallel ID_R , K_{PU})$) şifresini çözer ve U tarafından gönderilen ID_R ve N_{PU} değerlerini elde eder. Eğer elde etmiş olduğu N_{PU}' değeri ile ikinci adımda müşteriye kendisinin göndermiş olduğu N_{PU} değerleri aynı ise müşterinin kimliği kontrol edilmiş olur. Değerler farklı ise U'nun bir saldırgan olduğu anlaşılır. Daha sonra P, müşterinin kiminle iletişim kurduğunu anlamak için, müşterinin göndermiş olduğu ID_R bilgisini kontrol eder. Eğer müşterinin göndermiş olduğu ID_R bilgisi ile kasiyerin göndermiş olduğu ID_R bilgisi aynı ise kasiyerinde kimliği kontrol edilmiş oldur. Aksi durumda ise R'nin saldırgan olduğu anlaşılır.

4.2.1.3. Gizlice dinleme saldırısına karşı dayanıklılık

Saldırgan gizlice dinleme saldırısı yaparak iletişimi dinleyebilir. Ancak kullanıcılar arasında gönderilen gizli veriler şifreli olarak gönderildiği için, saldırganın gönderilen mesajların içeriğini elde etmesi mümkün olmayacaktır. Buna rağmen saldırgan iletişimi dinleyerek elde etmiş olduğu paketleri kullanarak yeniden gönderme saldırısını deneyebilir. Ancak bu saldırıda başarısız olacaktır. Saldırının detayları "yeniden gönderme saldırısı" başlığı altında anlatılmıştır.

4.2.1.4. Yeniden gönderme saldırısına karşı dayanıklılık

Her bir m-kupon için ayrı ayrı rasgele sayılar (N_{PU}, N_{FU} vb.) üretilmekte ve kuponların kullanım bilgileri F'nin veri tabanında saklanmaktadır. Ayrıca müşteri

kendi kimliğini ispatlamak için C_{ID} ve MUC değerlerinin özet değerini hesaplayıp ($\psi = H(MUC \parallel C_{ID})$) kupon sağlayıcı üzerinden (P) üretici firmaya (F) algoritmanın üçüncü adımında göndermektedir. Özet değeri ve rasgele sayı sayesinde F müşterinin kimliğini kontrol etmektedir. Bu kontrolün nasıl yapıldığı detaylı olarak kuponun oluşturulması aşamasında anlatılmıştır. Dolayısıyla saldırgan, daha önceki iletişimleri dinleyerek elde etmiş olduğu paketleri kullanarak algoritmanın doğal kullanıcılarını kandıramaz, yeniden gönderme saldırısı gerçekleştiremez. Saldırgan yine de elde etmiş olduğu paketleri tekrar göndermeyi denese bile sistemi kandıramaz, çünkü kuponların kullanım bilgileri veri tabanında tutulmaktadır.

4.2.1.5. Veri değiştirme saldırısına karşı dayanıklılık

İletişimin ve transfer edilen verilerin güvenliğini, gizlice dinleme ve ortadaki adam saldırılarından korumak için, algoritmada simetrik şifreleme, asimetrik şifreleme ve kontrol değerleri kullanılmıştır. Saldırganın gönderilen mesajların içeriğini değiştirebilmesi için ya kullanıcılardan birisinin gizli anahtarını bilmesi ya da şifreleme için kullanılan simetrik anahtarı bilmesi gerekmektedir. Dolayısıyla saldırganın bu anahtarlardan birisini bilmeden gönderilen paketlerin içeriğine müdahale etmesi mümkün olmayacaktır. Saldırgan yine de değiştirmeye çalışsa bile bu durum algoritmada kullanılan açık anahtarlı şifreleme sistemi ve kontrol amacıyla kullanılan rasgele sayılar sayesinde tespit edilecektir.

4.2.1.6. Yetkisiz kupon çoğaltma/üretme saldırısına karşı dayanıklılık

Müşterilere gönderilen m-kuponlar kişiye özel olarak gönderilmekte ve kime gönderildiyse C_{ID} değerleri üzerinden takip edilebilmektedir. Ayrıca müşteri, talep etmiş olduğu m-kuponun C_{ID} değeri ile birlikte MUC değerinin özet değerini almakta ($H(MUC \parallel C_{ID})$), almış olduğu bu özet değerini üretici firmaya (F) göndermektedir. C_{ID} değerleri veri tabanında saklanmakta, müşteri herhangi bir kuponu kullanmak istediği zaman bu değer veri tabanından kontrol edilmektedir. Bu nedenle herhangi bir şekilde bir m-kupon yeniden kullanılsa veya üretilse bu kontrollerde ortaya çıkacaktır.

4.2.1.7. Çoklu kupon kullanımı saldırısına karşı dayanıklılık

M-kuponların yeniden kullanılması mümkün değildir, çünkü m-kuponların kullanım bilgileri verilen indirimin geri alınması aşamasında veri tabanına kaydedilmekte ve bu bilgi kupon sağlayıcıya da (P) bildirilmektedir. Müşterinin kendisi bile bir kuponu tekrar kullanmak istese, bu durum kuponun kullanılması aşamasında yapılan kontrollerde ortaya çıkacak ve sistem indirimi onaylamayacaktır.

4.3. MCWCC'nin Scyther Aracı ile Yapılan Güvenlik Analizi

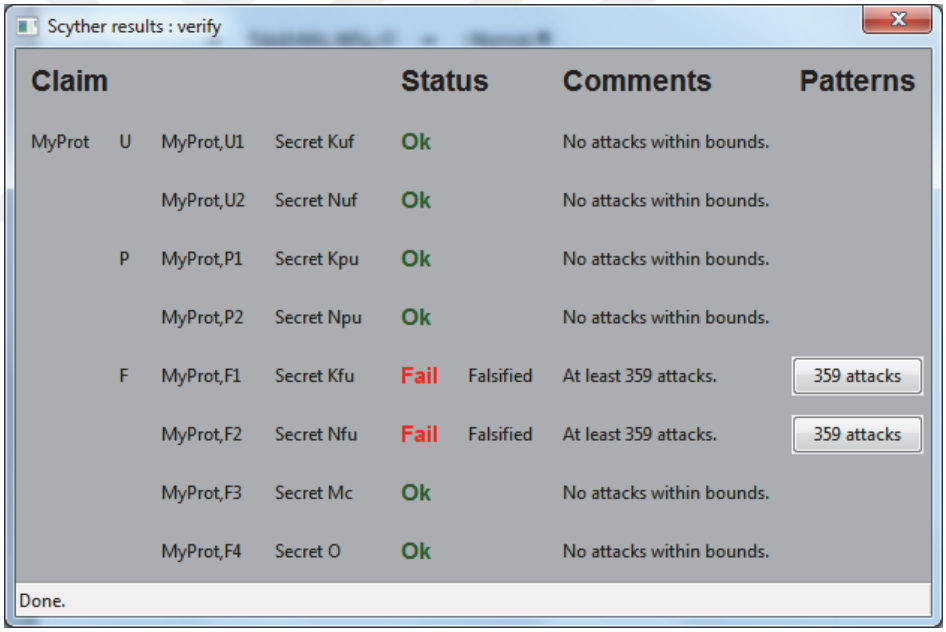
MCWCC'nin ne kadar güvenli olduğunu ve algoritmaya herhangi bir saldırının yapılamayacağını iddia etmiştik. Bu iddiamızı doğrulamak ve ispat etmek için önermiş olduğumuz algoritma olan MCWCC'yi Scyther v1.1.1 Windows versiyonu ile analiz ettik. Araç tarafından yapılacak olan güvenlik analizlerini başarı ile geçmek, istenilen tüm güvenlik kriterlerini sağlamak, hiç de kolay bir süreç olmayıp, uzun ve yoğun bir çalışma gerektirmektedir. Algoritmanın güvenliğinin tam olduğundan emin olmak ve Scyther tarafından tespit edilen açıkların kapatılması için algoritmanın her adımının yeniden gözden geçirilmesi gerekmektedir.

Analiz için her aşama birer birer kodlandı. Önce kuponun oluşturulması aşaması, sonra kuponun kullanılması aşaması ve en son verilen indirimin geri alınması aşaması. Her aşama kodlandıktan sonra ayrı ayrı araç ile analiz edildi. Bu çalışma her aşama araç tarafından doğrulanana kadar devam etti. Daha sonra, bir aşamada var olabilecek bir açık diğer aşamalarda da başka açıklara sebep olabileceği için algoritmanın tüm aşamalarının bir bütün olarak ele alınmasına karar verdik. Bu kapsamda MCWCC'un bir bütün olarak istenilen güvenlik kriterlerini sağlayıp sağlamadığını kontrol etmek için üç aşamayı da birlikte kodladık.

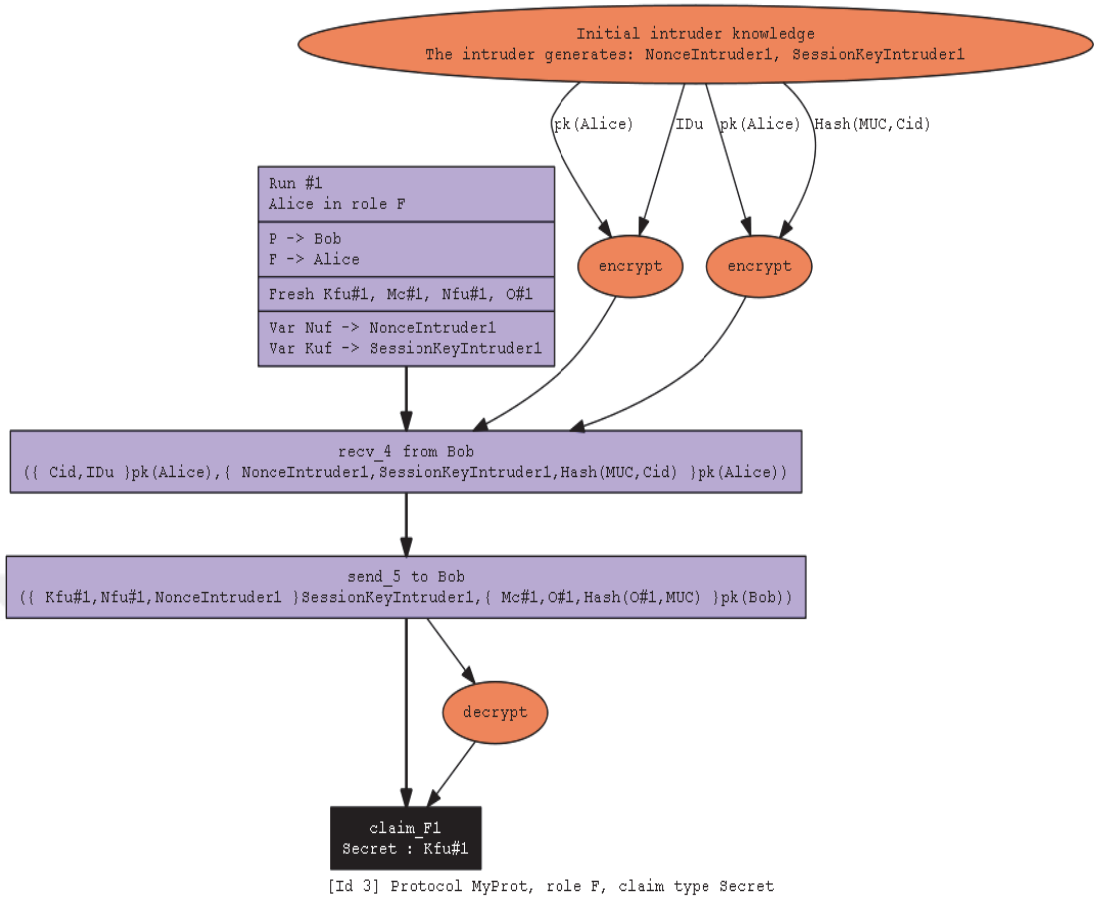
Altı adımdan oluşan kuponun oluşturulması aşaması Scyther Kullanım Kılavuzuna (Cremers, 2014) göre kodlandı. Kuponun kullanılması aşaması yedi adımdan oluşmaktadır. Bu aşama da kuponun oluşturulması aşaması gibi kodlandı ve değişkenler tanımlandı. MUC değeri özel bir değer olup sadece müşteri (U) ve üretici firma (F) tarafından bilinmektedir. Bu nedenle kodlarken MUC değeri k(U, F) şeklinde kodlandı. Bu gösterim MUC değerinin U ve F arasında paylaşılan gizli bir değer (Cremers, 2014) olduğunu göstermektedir. Kuponun oluşturulması aşamasının

kodlaması “send/receive” olayları şeklinde birden altıya kadar, kuponun kullanılması aşaması yediden on üçe kadar ve verilen indirimin geri alınması aşaması on dörtten on altıya kadar olan adımlar şeklinde verilmiştir.

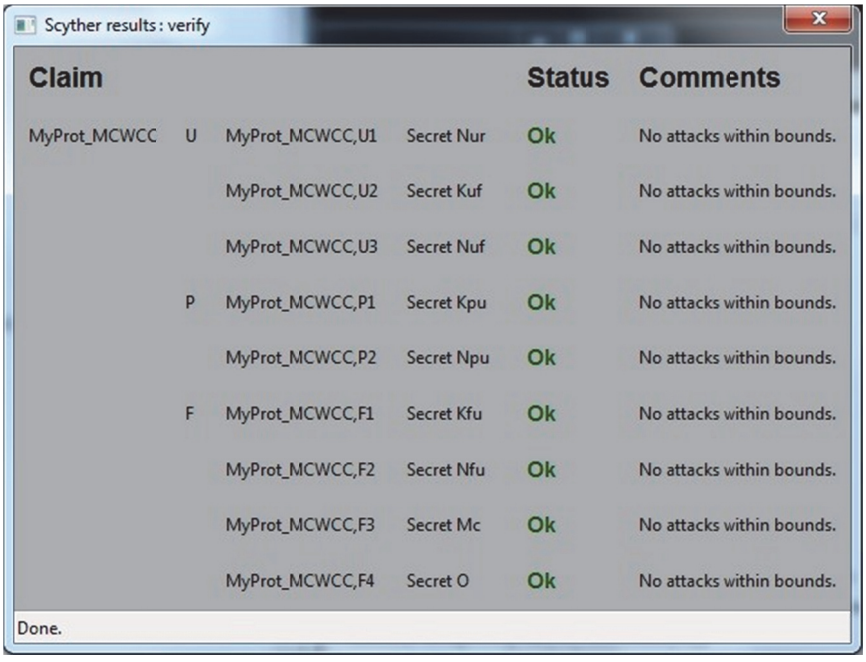
Scyther aracı yapılan ilk analizler sonucunda iki değer için 359 atak buldu. Yapılan ilk analiz sonucu Şekil 4.2’de ve tespit edilen saldırılardan birisi Şekil 4.3’te verilmiştir. Daha sonra algoritma üzerinde güncellemeler yapıldı güncellemeler tüm güvenlik kriterleri karşılanana ve hiç atak bulunmayana kadar devam etti. Yapılan uzun ve yoğun çalışma sonucunda MCWCC’nin güvenlik analizi tamamlandı ve Scyther aracı tarafından da MCWCC’ nin bir bütün olarak güvenli olduğu onaylanmış oldu. Yapılan analizin sonucu Şekil 4.4’te verilmiştir. Scyther aracı ile yapılan kodlama Ek-Ç’de verilmiştir. Scyther aracı için yazılan bu kod doğrudan aracın içine kopyalanıp yapıştırılarak test edilebilir.



Şekil 4.2. Algoritmanın ilk tasarım aşamalarında yapılan güvenlik analizi sonucu



Şekil 4.3. Scyter aracı tarafından bulunan algoritmaya yapılabilen bir saldırı



Şekil 4.4. MCWCC'un Scyther aracı ile yapılan analiz sonucu

5. TARTIŞMA

Yapılan bu çalışma ile hem müşterilerin hem de satıcıların m-kupon kullanımı konusunda yaşayabilecekleri tereddütleri gidermek ve güvenle kullanmalarını sağlamak hedeflenmiştir. Bu kapsamda da iki adet örnek algoritma seçilmiş ve bu algoritmaların güvenlik analizleri yapılmış, tespit edilen güvenlik açıklarına çözümler sunulmuştur. Eğer daha algoritmaların tasarım aşamasında bu hususa dikkat edilmiş ve güvenlik analizleri yapılmış olsaydı burada tespit edilen açıklar hiç ortaya çıkmayacak, kullanıcıların kafasında kişisel veri güvenlikleri ile ilgili soru işaretleri oluşmayacak, belki de m-kupon kullanımı çoktan yaygınlaşmış olacaktı.

M-kupon kullanımının yaygınlaşması ile ilgili dikkat edilecek hususların başında güvenlik gelse de tek unsur güvenlik değildir. Dickinger ve Klijen tarafından müşterilerin m-kupon kullanma istekleri ile ilgili bir çalışma yapılmıştır (Dickinger ve Kleijnen, 2008). Bu çalışmada, m-kuponların kullanımı için harcanan zaman ve enerjinin de kupon kullanımını doğrudan etkilediği gösterilmiştir. Eğer bir m-kuponu kullanmak için harcanan zaman artarsa kuponun kullanımı için olan istek azalmaktadır. Ayrıca yapılan çalışmada, müşterilerin spam'lere karşı korktukları ve kişisel güvenliklerinin tehlikede olabileceği endişesiyle m-kuponların kullanımı konusunda da ihtiyatlı oldukları görülmüştür. M-kuponların kullanımı konusunda bir başka araştırma Tercia ve Teicher tarafından yapılmıştır (Tercia ve Teichert, 2017). Yapmış oldukları çalışmada müşterilerin, ağızdan ağıza/kulaktan kulağa (word-of mouth - WOM) yöntemine tepkileri ve cinsiyetlerinin tercihlerine etkisi incelenmiştir.

M-kupon kullanımını etkileyecek diğer bir hususta NFC teknolojisinin kullanımının yaygınlaşmasıdır. Günümüzde temassız kartlar giderek daha fazla kullanılmaktadır. Bunlara örnek olarak kartların ulaşımda bilet olarak kullanılması verilebilir. Ayrıca bankalar tarafından verilen banka kartlarında yer alan temassız özelliği sayesinde işlemler giderek artan oranda temassız olarak yapılmakta, müşteriler tarafından geçmişte olduğundan çok daha fazla kullanılmaktadır. Bu noktada, temassız cihazların kullanımıyla ilgili kullanıcıların güvenlik kaygılarının birkaç yıl öncesine

kıyasla azaldığı, şirketlerin bu fırsattan faydalanarak m-kupon uygulamalarına daha fazla yöneleceği sonucuna kolaylıkla ulaşılabilir.

Dickinger ve Klijen tarafından yapılan çalışmada da (Dickinger ve Kleijnen, 2008) belirtildiği gibi burada dikkat edilmesi gereken en önemli nokta, firmaların müşterilerini m-kupon bombardımanına tutup onları boğamamalarıdır. Ayrıca firmalar müşterilerinin cinsiyeti, yaşı, sosyokültürel yapısı, sosyal çevresi, yaşadığı bölge, alışveriş alışkanlıkları gibi bilgileri analiz ederek doğru zamanda doğru indirimi yaparak müşterilerin dikkatini çekebilirler. Müşterilerin alışveriş oranlarının düştüğü dönemlerde onlara daha yüksek indirim oranları sunmak gibi.

6. SONUÇLAR VE ÖNERİLER

Mobil cihazlar hayatımızın bir parçası olması ile birlikte alışveriş alışkanlıkları da yeni bir boyuta taşınmış oldu. Bu kapsamda firmaların müşteri çekmek için kullandıkları yöntemler değişmekte, indirim için kullanılan kağıt bazlı kuponların yerini m-kuponlar almaktadır.

M-kuponlar sayesinde müşteriler güvenlik konusunda endişe yaşamadan, istemiş oldukları indirimi mobil cihazlarını sadece kasiyerin cihazına temas ettirerek elde edebilirler. Ayrıca firmalar müşterilerine verecekleri özel indirimleri kağıda basma/dağıtım/ulaştırma gibi ek maliyetleri düşünmeden, m-kupon kullanarak rahatlıkla yapabilirler. Buna ek olarak firmalar sadık müşterileri için kart basma ve bu kartları müşterilere ulaştırma maliyetlerinde de kurtulmakta, müşteriye ulaşmak için sadece mobil cihazlar yeterli olmakta, istediği zamanda istediği oranda indirimi sunarak müşterinin ilgisini sıcak tutma fırsatını elde etmektedirler.

Bu çalışmada, gelecekte yaygın olarak kullanılacağı değerlendirilen m-kupon algoritmalarının güvenlik analizini yapmak ve yeni ve güvenli bir m-kupon algoritması geliştirmek amacıyla, Hsueh ve Chen tarafından geliştirilen m-kupon algoritması (Hsueh ve Chen, 2010) ve Hsiang tarafından geliştirilen NFC tabanlı m-kupon algoritması (Hsiang, 2014) vaka analizi yapılmak üzere seçilmiş ve güvenlik analizleri yapılmıştır. Daha sonra Hsueh ve Chen algoritması ile Hsiang algoritmasının güvenlik analizlerinden elde ettiğimiz tecrübeler doğrultusunda yeni bir m-kupon algoritması geliştirilmiştir.

Hsueh ve Chen tarafından geliştirilen m-kupon algoritmasının (Hsueh ve Chen, 2010) hedef müşteri kitlesi için olan kısmının güvenlik analizi yapılmış, kuponun oluşturulması ve kuponun kullanılması aşamalarında güvenlik açıkları olduğu tespit edilmiştir. Kuponun oluşturulması aşamasındaki güvenlik açığı Eşitlik (2.5) ile gösterilen değerin P'nin açık anahtarı ile şifrelenerek gönderilmesi ile çözülmüştür Eşitlik (2.6). Kuponun kullanılması aşamasında ortadaki adam saldırısı gerçekleştirilmiş, çözüm olarak NFC teknolojisinin kullanılmasının yeterli olacağı

belirtilmiştir. Daha sonra kuponunun kullanılması aşamasında röle saldırısı gerçekleştirilmiş, bu saldırıyı önlemek için de sisteme onay kodu (O) eklenmiştir. Eklenen bu kod sayesinde müşteri gerçekten indirimi aldığını F'ye bildirmektedir. Önerilen algoritma Şekil 2.8'de verilmiştir.

Yapmış olduğumuz bu çalışma ile Şekil 2.6 ve Şekil 2.7'de gösterilen röle saldırılarının genel saldırılar olduğunu, bu saldırıların Dominikus ve Aigner tarafından sunulun m-kupon algoritması (Dominikus ve Aigner, 2007) gibi başka m-kupon algoritmalarına da rahatlıkla uyarlanabileceğini gördük.

Bu atak ayrıca Alshehri ve Briffa'nın, Dominikus ve Aigner'in geliştirmiş olduğu m-kupon algoritması (Dominikus ve Aigner, 2007) üzerinde yapmış olduğu güvenlik analizi (Alshehri ve diğ., 2013) sonucunda önerdikleri algoritmaya da rahatlıkla adapte edilebilir. Alshehri ve Briffa yapmış oldukları analiz ile bazı zayıf noktalar tespit ederek saldırılar gerçekleştirmiş, sonrasında da bu açıkları gidermek için çözüm önerisi sunmuşlardır. Önerdikleri yeni yapı ile güvenlik konusunda her ne kadar gelişme sağlamış olsalar da içeriden yapılan röle saldırısı hala yapılabilir durumdadır.

Hsiang tarafından geliştirilen algoritmanın (Hsiang, 2014) güvenlik analizi için, senaryolar, oyun kuramı, simülasyon yöntemi ve otomatik güvenlik algoritması doğrulama aracı Scyther kullanılmıştır. Hsiang tarafından geliştirilen m-kupon algoritmasının güvenlik analizi, ilk önce geliştirilen simülasyon aracılığıyla senaryolar üzerinden yapılmıştır. Senaryolarda saldırganla birlikte dört kullanıcı (müşteri, kupon sağlayıcı, kasiyer ve saldırgan) yer almış, saldırgan tüm iletişimi dinleyerek saldırıları gerçekleştirmiştir. Eğer saldırgan elde ettiği diğer kullanıcılara ait verilerle iletişimi manipüle edebiliyorsa saldırının başarılı olduğu aksi durumlarda ise algoritmanın güvenli olduğu anlaşılmıştır.

Bu çerçevede yapılan güvenlik analizi sonucunda; Hsiang tarafından, tüm güvenlik kontrollerinin m-kuponun kullanılması aşamasında yapıldığı, kuponların müşterilere ulaştırılması (kuponun oluşturulması) aşamasında herhangi bir güvenlik kontrolünün olmadığı, saldırıların da bu açık kullanılarak yapılabileceği gösterilmiştir. Bu açık sayesinde yetkisiz kişiler tarafından da kupon oluşturulabileceği, müşterilere verilen kuponların geçersiz yapılabileceği tespit edilmiştir.

Ayrıca Hsiang'ın iddia ettiği gibi algoritmanın, müşteri bilgilerinin gizliliğini sağlayamadığı, firmanın kendi içinde yapmış olduğu iletişimde kullandığı gizli anahtarın saldırgan tarafından ele geçirilebildiği de gösterilmiştir. Tespit edilen bu açıklar için çözüm önerileri sunulmuş, saldırılar tekrarlanarak önerilen sistemin kontrolü yapılmış, yapılan kontrol sonucunda saldırganın kullanıcılara (müşteri, kupon sağlayıcı, kasiyer) ait elde ettiği verilerle sistemi manipüle edemediği ve önerilen algoritmanın (Şekil 3.7) istenilen güvenlik düzeyini karşıladığı görülmüştür.

Daha sonra Hsiang tarafından geliştirilen algoritma, algoritma analiz aracı Scyther kullanılarak da analiz edilmiştir. Araç ile yapılan analiz sonuçları incelendiğinde oyun kuramı ve simülasyon yöntemi kullanılarak yapılan analiz sonuçları ile örtüştüğü görülmüştür. Algoritmada tespit edilen açıklar için sunulan çözüm önerileri de yine Scyther aracı ile tekrar analiz edilmiş ve önerilen yapının istenilen tüm güvenlik kriterlerini karşıladığı görülmüştür.

Burada önerilen algoritma, diğer m-kupon algoritmaları (Hsueh ve Chen, 2010; Dominikus ve Aigner, 2007; Hsiang ve Shih, 2009; Hsiang ve diğ., 2009; Park ve Lee, 2013; Hsiang, 2014; Chen ve diğ., 2016; Yim, 2016; Jiang ve diğ., 2016) ile karşılaştırıldığında, güvenlik konusunda öne çıkmaktadır. Çünkü Alshehri ve arkadaşları tarafından Dominikus ve Aigner'in çalışması (Dominikus ve Aigner, 2007) üzerinde yapılan analiz (Alshehri ve diğ., 2013) ile yine Alshehri tarafından tez çalışması olarak Hsiang ve arkadaşları tarafından yapılan çalışmalar (Hsiang ve Shih, 2009; Hsiang ve diğ., 2009) üzerinde yapılan analizler (Alshehri, 2015) dışında diğer m-kupon algoritmalarında güvenlik analizleri otomatik güvenlik algoritması doğrulama aracı kullanılarak yapılan bir çalışma bulunmamaktadır. Bu kapsamda burada önermiş olduğumuz yeni yapıda güvenlik açığı bulunmadığını ve aynı zamanda yapının uygulanabilir olduğunu rahatlıkla söyleyebiliriz.

Yapılan bu tez çalışması kapsamında elde edilen tecrübeler doğrultusunda m-kupon kullanımı için gerekli olan tüm güvenlik kriterlerini karşılayan yeni bir m-kupon algoritması MCWCC geliştirilmiştir. Geliştirilen algoritma MCWCC, güvenlik algoritmalarının doğrulanması amacıyla kullanılan ve çok güçlü bir araç olan Scyther analiz aracı ile analiz edilmiş, bu şekilde MCWCC'nin yüksek düzeyde güvenlik ve güvenilirliğe sahip olduğu doğrulanmıştır. Ayrıca bu çalışmada MCWCC'nin web

tabanlı simülasyonunu JavaScript kullanarak geliştirilmiş olup simülasyonun sözde kodları Ek-D'de verilmiştir.

Hem Alshehri ve arkadaşları tarafından, Dominikus ve Aigner'in birlikte geliştirdiği algoritmanın (Dominikus ve Aigner, 2007) güvenlik analizi (Alshehri ve diğ., 2013), hem Alshehri tarafından tez çalışması olarak yapılan (Alshehri, 2015) Hsiang ve arkadaşları tarafından geliştirilen özet tabanlı NFC m-kupon algoritmasının (Hsiang ve Shih, 2009) ve QR tabanlı NFC m-kupon algoritmasının (Hsiang ve diğ., 2009) güvenlik analizleri, hem de yapılan bu çalışma göstermektedir ki, geliştirilen tüm algoritma ve algoritmaların güvenlik analizlerinin tasarım aşamasında yapılması gerekmektedir. Burada asıl sorun, araştırmacılar tarafından geliştirilen algoritmaların çok azında güvenlik analizi için kullanılan yöntemden bahsedilmesidir. Genellikle tasarımı yapanlar kendi yorumları doğrultusunda tasarımlarının güvenli olduğunu iddia etmektedirler. Bu nedenle de güvenlik analizi yapılmamış bir sistemin güvenilir olup olmadığının kontrolünün başka araştırmacılar tarafından yapılması gerekmekte, bu da algoritmanın kabul görmesini geciktirmekte/engellemektedir.

Bu tez çalışması ile literatüre yapılmış olan katkıların detayları yukarıda sunulmuş olup yapılan katkılar üç ana başlık altında toplanabilir. Bahse konu katkıları temel olarak aşağıdaki şekilde özetleyebiliriz:

1. Geliştirilmesi planlanan sistem/algoritma/uygulamalara ait güvenlik analizi konusunun daha tasarım aşamasında düşünülmesi gereken bir husus olduğu gösterilmiştir. Bu kapsamda güvenlik analizi konusunda yapılan katkılar aşağıda sunulmuştur:

(i) M-kupon algoritmalarının güvenlik analizlerinin yapılması ve elde edilen sonuçlar ışığında, diğer sistem/algoritma/uygulamaların da güvenlik analizlerinin yapılmasının gerektiği,

(ii) Var olan algoritma/protokollerin de güvenlik analizlerinin yapılmasına ve analiz usullerine katkı sağlayacağı,

(iii) Analiz için birden fazla yöntemin (senaryo, simülasyon, algoritma güvenlik analiz aracı) kullanılmış olması da, algoritmaların dizayn aşamasında tasarıma farklı bakış açılarından (hem güvenlik hem de uygulanabilirlik) bakılmasına ve algoritmanın daha güvenilir olmasına katkı sağlayacağı.

(iv) Yeni tasarlanacak/geliştirilecek olan sistemlere/algoritmalara, bakış, analiz ve inceleme yöntemleri olarak rehberlik edeceği,

(v) Araştırmacılara, saldırı yöntemleri, saldırıların önlenmesi ve güvenlik analizi konusunda ışık tutacağı kanaatindeyiz.

2. Firmaların müşterilerine vereceği indirimler için güvenlik konusunda kaygı yaşamadan, istediği zaman istediği müşteriye, istediği oranda indirim sunabilmesini sağlayan m-kupon algoritmalarının güvenlik analizi yapılmıştır. Ayrıca yeni bir m-kupon algoritması MCWCC geliştirilerek güvenlik analizleri yapılmıştır. Böylelikle literatüre güvenlik analizleri yapılmış iki adet m-kupon algoritması ile yeni bir m-kupon algoritması kazandırılmıştır. Bu kapsamda yapılan temel katkılar aşağıda sunulmuştur:

(i) M-kupon algoritmalarının/uygulamalarının rahatlıkla kullanılabilmesi için güvenlik analizlerinin yapılması gerektiği gösterilmiş, bunun için de iki adet m-kupon algoritması (Hsueh ve Chen, 2010; Hsiang, 2014) seçilerek güvenlik analizleri yapılmıştır

(ii) Analiz sonucunda tespit edilen açıklar giderilerek algoritmalar güncellenmiş ve güvenlik analizleri yapılmıştır.

(iii) Güvenlik analizi için seçilen ilk algoritma olan Hsueh ve Chen tarafından geliştirilen m-kupon algoritmasının güvenlik analizi senaryolar üzerinden oyun kuramı kullanılarak yapılmıştır.

(iv) Hsiang tarafından geliştirilen m-kupon algoritmasının güvenlik analizi JavaScript kullanılarak geliştirilen web tabanlı simülasyon üzerinden oyun kuramı yöntemi ile yapılmıştır. Ayrıca algoritma güvenlik algoritmalarının doğrulanması için kullanılan Scyther aracı kullanılarak da analiz edilmiş, ardından önerilen çözümlerin başarılı olup olmadığı yine Scyther ile kontrol edilmiştir.

(v) Hsiang tarafından geliştirilen algoritmanın güvenlik analizi makale olarak hazırlanmış ve Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisinde yayınlanmak üzere kabul edilmiştir.

(vi) Yeni bir m-kupon algoritması MCWCC geliştirilmiş ve algoritmanın hem müşterilerin hem de satıcıların haklarını/güvenliğini yüksek seviyede garanti altına aldığı gösterilmiştir.

(vii) Güvenlik algoritmalarının doğrulanması için kullanılan Scyther aracı kullanılarak da MCWCC'nin güvenlik analizi yapılmış ve Scyther ile yapılan

analiz sonucunda algoritmanın tüm güvenlik kriterlerini karşıladığı ispat edilmiştir. Bu kapsamda hazırlanan makale yayınlanmak üzere Turkish Journal Of Electrical Engineering & Computer Sciences dergisince kabul edilmiş olup literatüre yeni bir m-kupon algoritması kazandırılmıştır.

3. Bu çalışmada yeni geliştirilen bir algoritmanın tasarımı ve güvenlik analizi yapılırken hangi yöntemlerin kullanılabileceği, uygulamalar ve örnekler ile birlikte sunulmuş olup kullanılan metodoloji aşağıda sunulmuştur:

(i) Güvenlik konusu tasarımın başından itibaren düşünülmüş ve MCWCC tasarlanırken güvenlik hep ön planda tutulmuştur.

(ii) MCWCC'nin tasarımı yapılırken saldırı senaryoları göz önünde bulundurulmuştur.

(iii) MCWCC'nin uygulanabilirliğinin analiz edilmesi için simülasyonu yapılmıştır.

(iv) Tasarımı tamamlandıktan sonra güvenlik analizi, oyun kuramı ve senaryolar üzerinden yapılmış, algoritmada tespit edilen açıklar için düzeltmeler yapılmıştır.

(v) En son aşamada algoritma aşama aşama, algoritmalarının doğrulanması için kullanılan Scyther aracı kullanılarak analiz edilmiş, araç tarafından tespit edilen açıklar için önlem alınmıştır.

Özetle yapılan bu tez çalışmasının, güvenli bir şekilde alışveriş yapılmasına olanak sağlayan m-kupon kullanımının yaygınlaşmasına katkı sağlanacağı ve yeni yapılacak çalışmaların/geliştirilecek algoritmaların güvenlik analizlerinin metodolojik olarak yapılmasına ışık tutacağı kanaatindeyiz.

KAYNAKLAR

Agarwal R.G.P.M.V., Modani N., An architecture for secure generation and verification of electronic coupons, *2001 USENIX Annual Technical Conference*, Boston, USA, 25-30 June 2001.

Aigner M., Dominikus S., Feldhofer M., A System of Secure Virtual Coupons Using NFC Technology, *5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, New York, USA, 19-23 March 2007.

Alshehri A., Briffa J.A., Schneide S., Wesemeyer S., Formal security analysis of NFC m-coupon protocols using Casper/FDR, *5th International Workshop on Near Field Communication (NFC)*, Zurich, Switzerland, 5 February 2013.

Alshehri A.A., NFC mobile coupon protocols: developing, formal security modelling and analysis, and addressing relay attack, PhD Thesis, University of Surrey, Guildford, 2015.

Anand R., Kumar M., Jhingran A., Distributing e-coupon on the Internet, *9th Annual Conference of the Internet Society*, San Jose, California, USA, 22-25 June 1999.

Arslan S., Demirel V., Kuru I., A public transport fare collection system with smart phone based NFC interface, *International Journal of Electronics and Electrical Engineering*, 2016, **4**(3), 258-262.

Bartoli A., Medvet E., An architecture for anonymous mobile coupons in a large network, *Journal of Computer Networks and Communications*, DOI: 10.1155/2016/2349148.

Basin D., Cremers C., Meier S., Provably repairing the ISO/IEC 9798 standard for entity authentication 1. *Journal of Computer Security*, 2013, **21**(6), 817-846.

Blundo C., Cimato S., Bonis AD., A lightweight protocol for the generation and distribution of secure e-coupons, *11th International Conference on World Wide Web,* New York, USA, 07-11 May 2002.

URL-1: https://people.cispa.io/cas.cremers/tools/protocols.html (Ziyaret tarihi: 02 Ocak 2019).

URL-2: https://people.cispa.io/cas.cremers/publications/index.html (Ziyaret tarihi: 02 Ocak 2019).

Chang C.C., Sun C.Y., A secure and efficient authentication scheme for E-coupon systems, *Wireless Personal Communications*, 2014, **77** (4), 2981-2996.

Chaudhary S., Garg N., Internet of things: a revolution, *Int J Adv Comput Technol*, 2014, **3**, 714-716.

Chen Y.Y., Tsai M.L., Chang F.J., The design of secure mobile coupon mechanism with the implementation for NFC smartphones, *Computers & Electrical Engineering*, 2016, **59**, 204-217.

Chincholle D., Eriksson M., Burden A., Location-sensitive services: it's now ready for prime time on cellular phones!. *The 4th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, London, England, 25-28 June 2002.

Cimato S., Bonis A.D., Online advertising: Secure E-coupons, Theoretical Computer Science. ICTCS 2001, *Lecture Notes in Computer Science*, 2001, 370-383, DOI: 10.1007/3-540-45446-2_24.

Cremers C., Horvat M., Improving the ISO/IEC 11770 standard for key management techniques, *International Journal of Information Security*, 2016, **15**(6), 659-673.

ISO/IEC 18092:2013: Information technology --Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1), *International Organization for Standardization*, 2013.

Cremers C.J., The scyther tool: Verification, falsification, and analysis of security protocols, *20th International Conference on Computer Aided Verification*, Princeton, NJ, USA, 7-14 July 2008.

Cremers C*., Scyther user manual,* Department of Computer Science, University of Oxford, Oxford, UK, 2014.

Cremers C., Key exchange in IPsec revisited: Formal analysis of IKEv1 and IKEv2, *16th European Symposium on Research in Computer Security*, Leuven, Belgium, 12-14 September 2011.

D'silva G.M., Scariah A.K., Pannapara L.R., Joseph J.J., Smart ticketing system for railways in smart cities using software as a service architecture, *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Coimbatore, India, 10 February 2017.

Danaher P.J., Smith M.S., Ranasinghe K., Danaher, T.S., Where, when, and how long: Factors that influence the redemption of mobile phone coupons, *Journal of Marketing Research*, 2015, **52**(5), 710-725.

Dickinger A., Kleijnen M., Coupons going wireless: Determinants of consumer intentions to redeem mobile coupons, *J Interact Mark*, 2008, **22**, 23-39.

Dominikus S., Aigner M., mCoupons: An application for near field communication (NFC), *21st International Conference on Advanced Information Networking and Applications Workshops,* Niagara Falls, Canada, 21-23 May 2007.

Evans D., *The internet of things how the next evolution of the internet is changing everything*, White Paper by Cisco Internet Business Solutions Group, 2012.

Feldhofer M., Dominikus S., Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm, *Lect Notes Comput Sc*, 2004, **4**, 357–370.

Finžgar L., Trebar M., Use of NFC and QR code identification in an electronic ticket system for public transport, *19th International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2011)*, Adriatic Islands Split, Croatia, 15-17 September 2011.

Ghìron S.L., Sposato S., Medaglia C.M., Moroni A., NFC ticketing: A prototype and usability test of an NFC-based virtual ticketing application, *1st International Workshop on Near Field Communication,* Hagenberg, Austria, 24-26 February 2009.

Goggin G., *Cell phone culture: Mobile technology in everyday life*, Routledge, New York, USA, 2012.

Gregoski M.J., Mueller M., Vertegel A., Shaporev A., Jackson B.B., Frenzel R.M., Treiber F.A., Development and validation of a smartphone heart rate acquisition application for health promotion and wellness telehealth applications, *International Journal of Telemedicine and Applications*, 2012, **2012** (1), 1-7.

GSM Association, *Mobile NFC Technical Guidelines-V2*, 2007.

Haselsteiner E., Breitfuß K., Security in near field communication (NFC), *Workshop on RFID Security*, Malaga, Spain, 11-13 July 2006.

Haraniya R., Sasmal C., Bopaliya B., Revar A., Comparative study of distributed online abatement, *International Journal of Computer Applications*, 2017, **165**(11), 25-28.

Hill S., Provost F., Volinsky F.C., Network-based marketing: Identifying likely adopters via consumer networks, *Statistical Science*, 2006, **21**(2), 256-276.

Hinarejos M.F., Isern-Deyà A.P., Ferrer-Gomila J.L., Huguet-Rotger L., Deployment and performance evaluation of mobile multicoupon solutions, *International Journal of Information Security*, 2019, **18**, 101-124.

Hinarejos M.F., Isern-Deyà A.P., Ferrer-Gomila J.L., Payeras-Capellà M., MC-2D: An Efficient and Scalable Multicoupon Scheme, *Comput J*, 2015, **58,** 758-778.

Hoare C.A.R., *Communicating Sequential Processes,* Prentice-hall, 1985.

Holton B., iPhone 6 and iOS 8: a look at accessibility with the help of iOS without the eye by Jonathan Mosen, *AFB AccessWorld Mag*, 2014, **15,** 10.

Hsiang H.C., A Secure and efficient authentication scheme for M-Coupon systems, *8th International Conference on Future Generation Communication and Networking (FGCN)*, Hainan, China, 20-23 December 2014.

Hsiang H.C., Kuo H.C., Shih W.K., A secure mCoupon scheme using Near Field Communication, *International Journal of Innovative Computing, Information and Control*, 2009, **5**(11), 3901-3909.

Hsiang H.C., Shih W.K., Secure mCoupons scheme using NFC, *International Conference on Business and Information*, Seoul, Korea, 7-9 July 2008.

Hsueh S.C., Chen J.M., Sharing secure m-coupons for peer-generated targeting via eWOM communications, *Electronic Commerce Research and Applications*, 2010, **9**, 283-293.

ISO/IEC 9798-3:1993, Information technology – Security techniques – Entity authentication mechanism – Part 3: Entity authentication using a public key algorithm, *International Organization for Standardization*, Genova, Switzerland, 1993.

Jakobsson M., Mackenzie P.D., Stern J.P., Secure and lightweight advertising on the web, *Comput Netw*, 1999, **31**, 1101-1109.

Jiang J., Zheng Y., Yuan X., Shi Z., Gui X., Wang C., Yao J., Towards secure and accurate targeted mobile coupon delivery, *IEEE Access*, 2016, **4**, 8116-8126.

Krishna S., Boren S.A., Balas E.A., Healthcare via cell phones: a systematic review, *Telemedicine and e-Health*, 2009, **15**(3), 231-240.

Kwapisz J.R., Weiss G.M., Moore S.A., Activity recognition using cell phone accelerometers, *ACM SigKDD Explorations Newsletter*, 2011, **12**(2), 74-82.

Lady E.L., *Chinese Remainder Theorem*, yayınlanmamış.

Mathews A.W., Yadron D., Health insurer anthem hit by hackers, The Wall Street Journal, http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720, (Yayın tarihi 04 Şubat 2015, Ziyaret tarihi: 02 Ocak 2019).

Montgomery P.L., A survey of modern integer factorization algorithms. *CWI quarterly*, 1994, **7**(4), 337-365.

Myerson R.B., *Game Theory*, Harvard University Press, 2013.

Ooi K.B., Tan G.W.H., Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card, *Expert Systems with Applications*, 2016, **59**, 33-46.

Özcanhan M.H., Dalkılıç G., Utku S., Cryptographically supported NFC tags in medication for better inpatient safety, *Journal of Medical Systems*, 2014, **38**(61), 1-15.

Park S.W., Lee I.Y., Efficient mcoupon authentication scheme for smart poster environment based on low-cost NFC, *International Journal of Security and Its Applications*, 2013, **7**(5), 131-138.

Park S.W., Lee I.Y., Light-Weight Authentication Scheme for NFC mCoupon Service in IoT Environments, *Advanced Multimedia and Ubiquitous Engineering*, 2016, **354**, 285-299.

Reinhart L., Naatus M.K., Groupon, m-commerce and mobile apps: Perceptions of small business owners and consumers, *Business & Entrepreneurship Journal*, 2017, **6**(1), 27-38.

Ryan P.Y.A., Schneider S.A., Goldsmith M., Lowe G., Roscoe A.W., *Modelling and analysis of security protocols*, Addison-Wesley Professional, 2001.

Saparkhojayev N., Nurtayev A., Baimenshina G., Access Control and Management System Based on NFC-Technology by the Use of Smart Phones as Key, *Middle East J*, 2014, **21**(7), 1130-1135.

Schäfer G., Kreisel A., Rummler D., Stopka U., Development of a concept for evaluation user acceptance and requirements for NFC based e-ticketing in public transport, *19th International Conference on Human-Computer Interaction*, Vancouver, Canada, 9-14 July 2017.

Shojima T., Ikkai Y., Komoda N., A method for mediator identification using queued history of encrypted user information in an incentive attached peer to peer electronic coupon system, *IEEE International Conference on Systems, Man and Cybernetics*, The Hague, Netherlands, 10-13 October 2004.

Taha A.M., Abdel-Hamid A.T., Tahar S., Formal verification of IEEE 802.16 security sublayer using Scyther tool, *International Conference on Network and Service Security,* Paris, France, 24-26 June 2009.

Tan G.W.H., Ooi K.B., Chong S.C., Hew T.S., NFC mobile credit card: the next frontier of mobile payment?, *Telemat Informat*, 2014, **31**, 292-307.

Tang Q., Zhao X., Liu S., The effect of intrinsic and extrinsic motivations on mobile coupon sharing in social network sites: The role of coupon proneness, *Internet Res*, 2016, **26**, 101-119.

Tercia C.Y., Teichert T., How consumers respond to incentivized word of mouth: An examination across gender, *Austr Mar J*, 2017, **25**, 46-56.

Vives-Guasch A., Payeras-Capellà M.M., Macia M.P., Castellà-Roca J., Ferrer-Gomila J.L., A secure e-ticketing scheme for mobile devices with near field communication (NFC) that includes exculpability and reusability, *IEICE T Inf Syst*, 2012, **95**, 78-93.

Yıldırım K., Uçar G., Keskin T., Kavak A., Fall detection using smartphone-based application, *International Journal of Applied Mathematics, Electronics and Computers*, 2016, **4**(4), 140-144.

Yim J., Design of a smart coupon system, *Multimedia and Ubiquitous Engineering*, 2016, **11**(3), 187-198.

Zhang M., Yao D., Zhou Q., The application and design of QR code in scenic spot's eTicketing system-a case study of shenzhen happy valley, *Sci Technology*, 2012, **2**, 817-822.

Zhao X., Tang Q., Liu S., Liu F., Social capital, motivations, and mobile coupon sharing, *Ind Manage Data Syst*, 2016, **116**, 188-206.

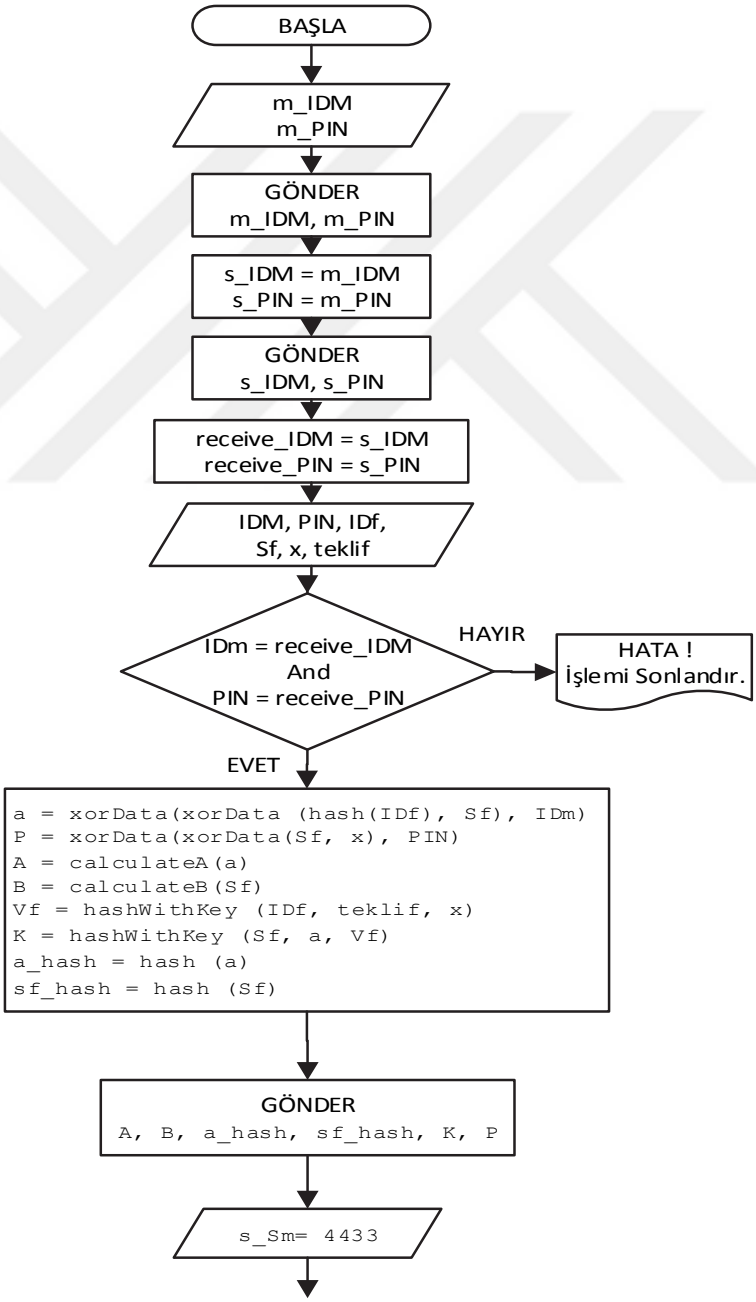
Zhu H., Xia Y., Li H., An efficient and secure biometrics-based one-time identity-password authenticated scheme for e-coupon system towards mobile internet, *Journal of Information Hiding and Multimedia Signal Processing*, 2015, **6**(3), 444-457.

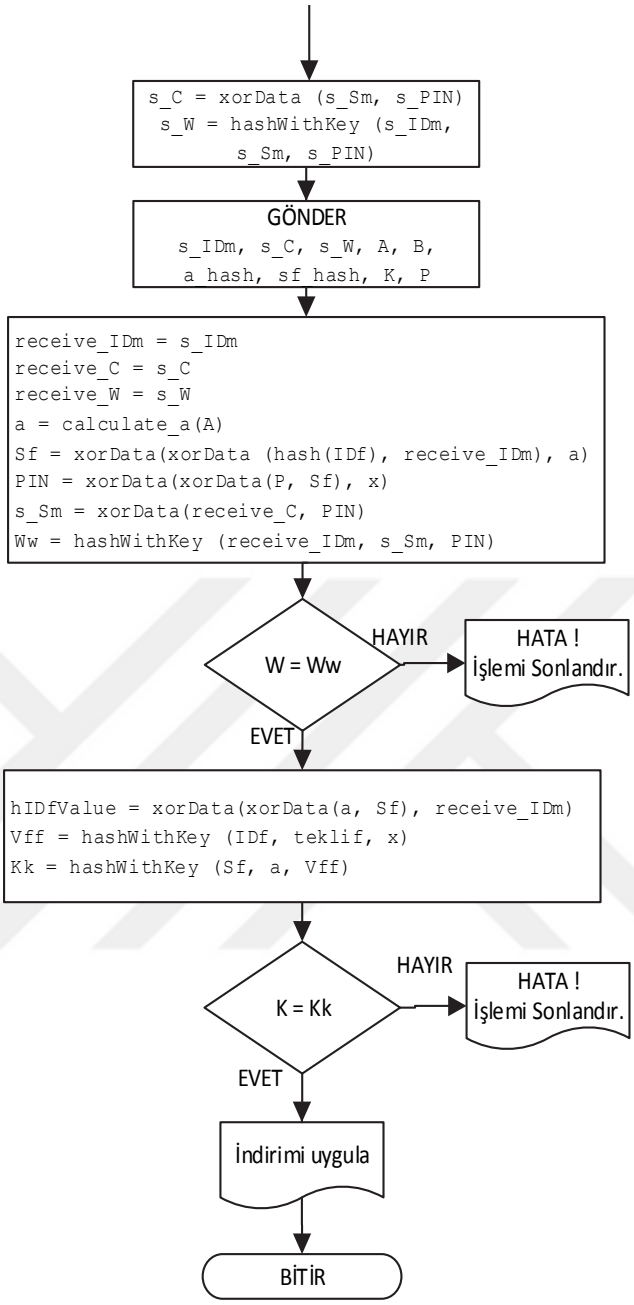
EKLER

Ek-A

Müşterinin bilgilerinin çalınması ve yetkisiz kupon kullanma/üretme saldırılarına ait simülasyonun sözde kodları

Algoritmanın test edilebilmesi için simülasyon web tabanlı bir uygulama olarak tasarlanmış ve algoritma analiz edilmiştir. Aşağıda programın akış diyagramı ve sözde kodları verilmiştir.




s_C = xorData (s_Sm, s_PIN)
s_W = hashWithKey (s_IDm, s_Sm, s_PIN)
GÖNDER
s_IDm, s_C, s_W, A, B, a hash, sf hash, K, P
receive_IDm = s_IDm
receive_C = s_C
receive_W = s_W
a = calculate_a(A)
Sf = xorData(xorData (hash(IDf), receive_IDm), a)
PIN = xorData(xorData(P, Sf), x)
s_Sm = xorData(receive_C, PIN)
Ww = hashWithKey (receive_IDm, s_Sm, PIN)
W = Ww
HAYIR
HATA ! İşlemi Sonlandır.
EVET
hIDfValue = xorData(xorData(a, Sf), receive_IDm)
Vff = hashWithKey (IDf, teklif, x)
Kk = hashWithKey (Sf, a, Vff)
K = Kk
HAYIR
HATA ! İşlemi Sonlandır.
EVET
İndirimi uygula
BİTİR

Simülasyonun sözde kodları

```
// Müşterinin kimlik bilgilerinin çalınması (Impersonation attack)
// yetkisiz kupon kullanma (unauthorized coupon copying/generation)
// saldırılarının başlangıcı

// user: MUSTERI
// Müşterinin yapmış olduğu işlemler
      // Müşterinin ID değeri
      m_IDm = 1111;
      // Müşterinin PIN değeri
      m_PIN = 1234;
      sendValue (m_IDm, m_PIN)
// M-kupon talebi için gönderilen veriler. Bu bilgiler farkında
//  olmadan doğrudan saldırgana gönderiliyor ve saldırgan bu
bilgileri
// daha sonra kullanmak üzere saklıyor.

// user: SALDIRGAN
// Saldırganın yapmış olduğu işlemler
      // Saldırgan müşteriden elde etmiş olduğu m_IDm= 1111 değerini
      // kendi ID değeri olarak kullanıyor.
      s_IDm = m_IDm;
      // Saldırgan müşteriden elde etmiş olduğu m_PIN= 1234 değerini
      // kendi PIN değeri olarak kullanıyor.
      s_PIN = m_PIN;

      // Bu bilgiler saldırgan tarafından kupon sağlayıcıya
      // gönderiliyor. Amaç yeni bir m-kupon elde etmek
      sendValue (s_IDm, s_PIN)

// Müşterinin kimlik bilgilerinin çalınması saldırısının sonu
// (Impersonation attack)

// user: KUPON_SAĞLAYICI
// Kupon sağlayıcının yapmış olduğu işlemler
      // Saldırgandan gelen bilgiler
      receive_IDm = s_IDm;
      // Saldırgandan gelen bilgiler
```

```
      receive_PIN = s_PIN;
      // Kupon sağlayıcının veri tabanında kayıtlı olan
      // müşterinin ID değeri
      IDm = 1111;
      // Kupon sağlayıcının veri tabanında kayıtlı olan
      // müşterinin PIN değeri
      PIN = 1234;
      // Kupon sağlayıcının ID değeri
      IDf= 2222;
      // Kupon sağlayıcının kupon için üretmiş olduğu rasgele sayı
      Sf= 6543;
      // Kupon sağlayıcının kurum için haberleşmede kullanmış
      // olduğu gizli anahtar
      x= 9876;
      // Kuponun indirim oranı
      teklif= 25;

      if (IDm == receive_IDm && PIN == receive_PIN) {alert ("MUSTERI
ONAYLANDI")}
         else {alert ("Uzgunum!!! MUSTERI GECERLI DEGIL.");
             throw new Error('Uygulama sonlandırıldı !!!') }

      // a değeri hesaplanıyor
      a = xorData(xorData (hash(IDf), Sf), IDm)
      // P değeri hesaplanıyor
      P = xorData(xorData(Sf, x), PIN)
      // A değeri hesaplanıyor
      A = calculateA(a)
      // B değeri hesaplanıyor
      B = calculateB(Sf)
// Burada yapılan işlem (A ve B değerlerinin elde edilmesi) her ne
// kadar açık anahtarlı şifreleme ise de açık anahtarın bir parçası
// olan n değerinin sadece firma tarafından bilinmesi nedeniyle
// fonksiyon olarak gösterilmiştir. Bu fonksiyonda "a" değeri
// şifrelenerek "A" değeri elde edilmektedir.

      // Vf değeri hesaplanıyor
      Vf = hashWithKey (IDf, teklif, x)
      // K değeri hesaplanıyor
      K = hashWithKey (Sf, a, Vf)
```

```
      // a_hash değeri hesaplanıyor
      a_hash = hash (a)
      // sf_hash değeri hesaplanıyor
      sf_hash = hash (Sf)
      // M-kupon bilgisi farkında olmadan doğrudan saldırgana
      // gönderiliyor
      sendValue (A, B, a_hash, sf_hash, K, P)


// user: SALDIRGAN
// Saldırganın yapmış olduğu işlemler
      // Saldırgan kullanacağı rasgele sayı
      s_Sm= 4433;
      // Saldırgan s_C değerini hesaplıyor
      s_C = xorData (s_Sm, s_PIN)
      // Saldırgan s_W değerini hesaplıyor
      s_W = hashWithKey (s_IDm, s_Sm, s_PIN)
      // Saldırgan bu değerleri kasiyere gönderiyor.
      sendValue (s_IDm, s_C, s_W, A, B, a_hash, sf_hash, K, P)


// user: KASIYER
// Kasiyerin yapmış olduğu işlemler
      // Saldırgandan gelen bilgiler
      receive_IDm = s_IDm;
      // Saldırgandan gelen bilgiler
      receive_C = s_C;
      // Saldırgandan gelen bilgiler
      receive_W = s_W;
      // a değerini gelen A değerinden hesaplıyor
      a = calculate_a(A)
//  Burada  kasiyer  gizli  anahtarını  kullanarak  "A"  değerinin
şifresini
// çözmektedir. Şifreleme işleminde olduğu gibi burada da şifreleme
// işlemi fonksiyon olarak gösterilmiştir.
      // Sf değerini hesaplıyor
      Sf = xorData(xorData (hash(IDf), receive_IDm), a)
      // PIN değerini hesaplıyor
      PIN = xorData(xorData(P, Sf), x)
      // s_Sm değerini hesaplıyor
```

```
      s_Sm = xorData(receive_C, PIN)
      // Ww değerini hesaplıyor
      Ww = hashWithKey (receive_IDm, s_Sm, PIN)
      // Elde edilen değerler karşılaştırılıyor
      if (W = Ww) { alert ("DEGERLER AYNI")}

            else {alert ("Uzgunum!!! KUPON GECERLI DEGIL.");
                  throw new Error(' Uygulama sonlandırıldı !!!') }
      // hIDfValue değerini hesaplıyor
      hIDfValue = xorData(xorData(a, Sf), receive_IDm)
      // Vff değerini hesaplıyor
      Vff = hashWithKey (IDf, teklif, x)
      // Kk değerini hesaplıyor
      Kk = hashWithKey (Sf, a, Vff)
      // Elde edilen değerler karşılaştırılıyor
      if (K = Kk) {alert ("KUPON GECERLI, INDIRIM UYGULANDI")}

            else {alert ("Uzgunum!!! KUPON GECERLI DEGIL.");
                  throw new Error(' Uygulama sonlandırıldı !!!')}
            // Bu aşamaya kadar sorun yoksa kasiyer indirimi
            // uyguluyor.
// Yetkisiz kupon kullanma/üretme saldırısının sonu
// (unauthorized coupon copying/generation)
```

Ek-B

Hsiang tarafından geliştirilen algoritmanın Scyther aracı için yazılan kodları

Hsiang tarafından geliştirilen algoritmanın Scyther aracı ile test edilebilmesi için Scyther kılavuzuna göre hazırlanan SPDL (tanımlama ve açıklama dili - specification and description language) kodları aşağıda sunulmuştur. Bu kodlar doğrudan araca kopyalanarak çalıştırılabilir.

```
// Hsiang_algoritmasi.spdl

hashfunction Hash;
usertype SessionKey;
usertype String;

protocol MyProt(M, F)

{
role M {
      fresh IDm, PIN          : String;
      var A, B                : String;
      var IDf, Sf, x, a, Vf   : String;
      fresh Sm                : Nonce;

      send_1(M, F, IDm, PIN);
            recv_2( F, M, A, B, Hash ({{Hash (IDf)} Sf } IDm ), Hash
(Sf), {Sf, a} Vf, { {Sf} x} PIN );
      send_3 ( M, F, IDm, {Sm}PIN, {IDm, Sm} PIN, A, B, Hash ({{Hash
(IDf)} Sf } IDm ), Hash (Sf), {Sf, a} Vf, { {Sf} x} PIN );

      claim_M1(M, Secret, PIN);
      claim_M2(M, Secret, IDf);
      claim_M3(M, Secret, Sf);
      claim_M4(M, Secret, x);
      claim_M5(M, Secret, a);
  }
```

```
role F {
      var IDm, PIN                  : String;
      fresh A, B                    : String;
      fresh IDf, Sf, x, a, Vf       : String;
      var Sm                        : Nonce;

            recv_1(M, F, IDm,PIN);
      send_2 ( F, M, A, B, Hash ({{Hash (IDf)} Sf } IDm ), Hash
(Sf), {Sf, a} Vf, { {Sf} x} PIN );
            recv_3 ( M, F, IDm, {Sm}PIN, {IDm, Sm} PIN, A, B, Hash
({{Hash (IDf)} Sf } IDm ), Hash (Sf), {Sf, a} Vf, { {Sf} x} PIN );

      claim_F1(F, Secret, PIN);
      claim_F2(F, Secret, IDf);
      claim_F3(F, Secret, Sf);
      claim_F4(F, Secret, x);
      claim_F5(F, Secret, a);
  }
}
```

Ek-C

Saldırılara karşı önerilen algoritmanın Scyther aracı için yazılan kodları

Hsiang tarafından geliştirilen algoritmaya yönelik olarak yapılan saldırıları engellemek için önerilen algoritmanın Scyther aracı ile test edilebilmesi için Scyther kılavuzuna göre hazırlanan SPDL (tanımlama ve açıklama dili - specification and description language) kodları aşağıda sunulmuştur. Bu kodlar doğrudan araca kopyalanarak çalıştırılabilir.

```
// Hsiang_algoritmasi_onerilen_hali.spdl
hashfunction Hash;
usertype SessionKey;
usertype String;

protocol MyProt(M, F)
{
role M {
      fresh IDm, PIN          : String;
      var A, B                : String;
      var IDf, Sf, x, a, Vf   : String;
      fresh Nm, Sm            : Nonce;
      var Nf                  : Nonce;

      send_1(M,F, IDm, Nm);
            recv_2(F,M, {{Nm, Nf} sk(F)} pk(M));
      send_3(M, F, {{Nf, PIN} sk(M) } pk(F));
            recv_4( F, M, A, B, Hash ({{Hash (IDf)} Sf } IDm ), Hash
(Sf), {Sf, a} Vf, { {Sf} x} PIN );
      send_5 ( M, F, IDm, {Sm}PIN, {IDm, Sm} PIN, A, B, Hash ({{Hash
(IDf)} Sf } IDm ), Hash (Sf), {Sf, a} Vf, { {Sf} x} PIN );

      claim_M1(M, Secret, PIN);
      claim_M2(M, Secret, IDf);
      claim_M3(M, Secret, Sf);
      claim_M4(M, Secret, x);
      claim_M5(M, Secret, a);
  }
```

```
role F {
      var IDm, PIN            : String;
      fresh A, B              : String;
      fresh IDf, Sf, x, a, Vf : String;
      var Nm, Sm              : Nonce;
      fresh Nf                : Nonce;

            recv_1(M,F, IDm,Nm);
      send_2(F,M, {{Nm, Nf} sk(F)} pk(M));
            recv_3(M, F, {{Nf, PIN} sk(M) } pk(F));
      send_4 ( F, M, A, B, Hash ( { {Hash (IDf)} Sf } IDm ), Hash
(Sf), {Sf, a} Vf, { {Sf} x} PIN );
            recv_5 ( M, F, IDm, {Sm}PIN, {IDm, Sm} PIN, A, B, Hash (
{ {Hash (IDf)} Sf } IDm ), Hash (Sf), {Sf, a} Vf, { {Sf} x} PIN );

      claim_F1(F, Secret, PIN);
      claim_F2(F, Secret, IDf);
      claim_F3(F, Secret, Sf);
      claim_F4(F, Secret, x);
      claim_F5(F, Secret, a);
  }
}
```

Ek-Ç

MCWCC'nin Scyther aracı için yazılan kodları (MCWCC.spdl)

```
// Onay kodlu m-kupon algoritmasi(M-coupon Protocol with
// Confirmation Code (MCWCC))

hashfunction Hash;
usertype SessionKey;
usertype String;
const IDu, IDp, IDf, IDr  : String;

protocol MyProt-MCWCC (U,P, F, R)
{

 role U {
   fresh Nup, Nuf, Nur  : Nonce;
   fresh Cid            : String;
   var Npu, Nfu, O      : Nonce;
   fresh Kuf            : SessionKey;
   var Kpu, Kfu         : SessionKey;

   send_1(U,P, IDu,Nup);
      recv_2(P,U, IDp, {{Nup,Npu,Kpu}sk(P)} pk(U));
   send_3(U,P, {{Nuf, Kuf, Hash (k(U, F), Cid)}pk(F), Npu,Cid} Kpu);
      recv_6(P,U, {Kfu, Nfu, Nuf} Kuf);
   send_7(U,R, IDu, Nur);
      recv_8(R,U, IDr, {Nur}sk(R));
   send_9(U,R, {Npu, IDr}Kpu, Cid);
      recv_12(R,U,  Hash (O, k(U, F)), {Nup, O} Kpu);
   send_13(U,R, {O, Nfu} Kfu);

   claim_U1(U, Secret, Nur);
   claim_U2(U, Secret, Kuf);
   claim_U3(U, Secret, Nuf);
}
```

```
 role P {
   fresh Npu                  : Nonce;
   var Nup, Nuf, O, Mc, Nfu   : Nonce;
   var Cid                    : String;
   fresh Kpu                  : SessionKey;
   var Kuf, Kfu               : SessionKey;

      recv_1(U,P, IDu,Nup);
   send_2(P,U, IDp, {{Nup,Npu,Kpu}sk(P)} pk(U));
      recv_3(U,P, {{Nuf, Kuf, Hash (k(U, F), Cid)}pk(F), Npu,Cid}
Kpu);
   send_4(P,F, {Cid, IDu} pk(F), {Nuf,Kuf,Hash (k(U, F), Cid)}k(P,
F));
      recv_5(F,P, {Kfu, Nfu, Nuf} Kuf, {Mc, O, Hash (O, k(U,
F))}pk(P));
   send_6(P,U, {Kfu, Nfu, Nuf} Kuf);
      recv_10(R, P,  {{{Npu, IDr}Kpu, IDu} sk(R), IDr} pk(P));
   send_11(P,R, {Hash (O, k(U, F)), {Nup, O} Kpu, Mc}pk(R));
      recv_16(F,P, {{Cid}sk(F)}pk(P));

   claim_P1(P, Secret, Kpu);
   claim_P2(P, Secret, Npu);
}

 role F {
   fresh Kfu            : SessionKey;
   var Kuf              : SessionKey;
   var Cid              : String;
   fresh Mc, Nfu, O     : Nonce;
   var Nuf, Nup         : Nonce;
   var Kpu              : SessionKey;

      recv_4(P,F, {Cid, IDu}pk(F), {Nuf,Kuf,Hash (k(U, F),Cid)}k(P,
F));
   send_5(F,P, {Kfu, Nfu, Nuf} Kuf, {Mc, O, Hash (O, k(U,
F))}pk(P));
      recv_14(R,F, {Cid, {Hash (O, k(U, F))}sk(R), {Nup, O}
Kpu}pk(F));
// send_15(F,R, OKAY);              //this is OKAY message to R
   send_16(F,P, {{Cid}sk(F)}pk(P));
```

```
   claim_F1(F, Secret, Kfu);
   claim_F2(F, Secret, Nfu);
   claim_F3(F, Secret, Mc);
   claim_F4(F, Secret, O);
}


 role R {
   var Kfu, Kpu                    : SessionKey;
   var Cid                         : String;
   var Nup, Nur, Npu, Mc, O, Nfu   : Nonce;

      recv_7(U,R, IDu, Nur);
   send_8(R,U, IDr, {Nur}sk(R));
      recv_9(U,R, {Npu, IDr}Kpu, Cid);
   send_10(R, P,  {{{Npu, IDr}Kpu, IDu} sk(R), IDr} pk(P));
      recv_11(P,R, {Hash (O, k(U, F)), {Nup, O} Kpu, Mc}pk(R));
   send_12(R,U,  Hash (O, k(U, F)), {Nup, O} Kpu);
      recv_13(U,R, {O, Nfu} Kfu);
   send_14(R,F, {Cid, {Hash (O, k(U, F))} sk(R), {Nup, O} Kpu}
pk(F));
//    recv_15(F,R, OKAY);              //this is OKAY message to R
 }
}
```

Ek-D

MCWCC simülasyonunun sözde kodları

```
variable: KUu, KUp, KUf, KUr   // public keys of participants
variable: KRu, KRp, KRf, KRr   // private keys of participants
variable: IDu, IDp, IDf, IDr   // ID values of participants
// -- THE ISSUING PHASE -- //
user: USER (U)      //STEP 1
 variable: MUC      // shared secret value between U and F to identify the U
 variable: Nup, Nuf, Nur // Nonce values defined by U
 variable: Cid           // m-coupon id
 variable: Kuf          // symmetric key: defined by U and will be used by F
 output: IDu : Nup      // IDu and Nup values are sent to P

user: COUPON_PROVIDER (P) //STEP 2
 variable: Npu          // Nonce values defined by P
 variable: Kpu          // symmetric key: defined by P and will be used by U
 equation: step_2_a = concatenate (Nup, Npu, Kpu);
 equation: step_2_b = encWithKU ((signWithKR (step_2_a, KRp), KUu)
                          //first symmetric then asymmetric encryption
 output: IDp : step_2_b       // IDp and step_2_b values are sent to U

user: USER (U)        //STEP 3
 equation: decWithKR (step_2_b, KRu);             //asymmetric decryption
 equation: if (Nup' == Nup) {continue} else {abort MCWCC};
 equation: step_3_a = concatenate (Nuf, Kuf);
 equation: control_hash_value = hash (concatenate (MUC, Cid));
 equation: step_3_b = concatenate (step_3_a, control_hash_value);
 equation: step_3_c = encWithKU (step_3_b, KUf);   //asymmetric encryption
 equation: step_3_d = concatenate (step_3_c, concatenate (Npu, Cid));
 equation: step_3_e = encDecWithKey (step_3_d, Kpu); //symmetric encryption
 output: step_3_e     // step_3_e value is sent to P

user: COUPON_PROVIDER (P)  //STEP 4
 equation: encDecWithKey (step_3_e, Kpu);       //symmetric decryption
 equation: if (Npu' == Npu) {continue} else {abort MCWCC};
 equation: step_4_a = encWithKU (concatenate (Cid, IDu), KUf);
 output: step_4_a : step_3_c // values are sent to F

user: MANIFACTURER (F)      //STEP 5
 variable: Kfu       // symmetric key: defined by F and will be used by U
 variable: MC        // discount info
 variable: Nfu       // Nonce value defined by F
 variable: O         // Control value
 variable: MUC      // shared secret value between U and F to identify the U
 equation: decWithKR (step_4_a, KRf);  //asymmetric decryption
 equation: decWithKR (step_3_c, KRf);  //asymmetric decryption
```

```
 equation: incoming_hash = control_hash_value;
                          // this value is calculated at the third step by U
 equation: hash_value = hash (concatenate (MUC, Cid') // this value
          // is calculated by F using stored MUC value and sent Cid' value
 equation: if (hash_value == incoming_hash) {continue} else {abort MCWCC};
 equation: step_5_a = concatenate (Kfu, Nfu, Nuf);
 equation: step_5_b = encDecWithKey (step_5_a, Kuf);
 equation: step_5_c = concatenate (Mc, O, hash (concatenate (O, MUC));
 equation: step_5_d = encWithKU (step_5_c, KUp);
 output: step_5_b : step_5_d

user: COUPON_PROVIDER (P)  //STEP 6
 equation: decWithKR (step_5_d, KRp);
 output: step_5_b

user: USER (U)
 equation: encDecWithKey (step_5_b, Kuf);
 equation: if (Nuf' == Nuf) {issuing phase is completed} else {abort MCWCC};
// issuing phase is completed

// -- THE REDEMPTION PHASE -- //

user: USER (U)       //STEP 7
 variable: Nur           // Nonce value defined by U
 output: IDu : Nur

user: RETAILER (R)         //STEP 8
 equation: step_8 = signWithKR (Nur, KRr);
 output: IDr : step_8

user: USER (U)       //STEP 9
 equation: if (Nur' == Nur) {continue} else {abort MCWCC};  //The Nur value
                // sent by U and The Nur' sent by R are controlled
 equation: step_9 = encDecWithKey (concatenate (Npu, IDr), Kpu);
 output: step_9 : Cid

user: RETAILER (R)       //STEP 10
equation: step_10_a = signWithKR (concatenate (step_9, Cid, IDu), KRr)
equation: step_10_b = encWithKU (concatenate (step_10_a, IDr), KUp)
output: step_10_b

user: COUPON_PROVIDER (P)   //STEP 11
 equation: decWithKR (step_10_b, KRp);
 equation: encDecWithKey (step_9, Kpu);
 equation: if (IDr' == IDr) {continue} else {abort MCWCC};  //The IDr value
                       // sent by U and The IDr sent by R are controlled
 equation: if (Npu' == Npu) {continue} else {abort MCWCC};  //The stored Npu
                       // value and the sent value by U are controlled
 equation: step_11_a = hash (concatenate (O, MUC));
```

```
 equation: step_11_b = encDecWithKey (concatenate (Nup, O), Kpu);
 equation: step_11_c = encWithKU(concatenate(step_11_a,step_11_b, Mc), KUr);
 output: step_11_c

user: RETAILER (R)   //STEP 12
 equation: decWithKR (step_11_c, KRr);
 output: step_11_a : step_11_b

user: USER (U)   //STEP 13
 equation: encDecWithKey (step_11_b, Kpu);
 equation: if (Nup' == Nup) {continue} else {abort MCWCC};  //The stored Nup
         // value and the sent value by P are controlled
 equation: step_13_a = hash (concatenate (O', MUC));  // hash value is
         // recalculated by using the stored MUC value and received O' value
 equation: if (step_13_a == step_11_a) {continue} else {abort MCWCC};
         // Calculated hash value and received hash value are controlled
 equation: step_13_b = encDecWithKey (concatenate (O, Nfu), Kfu);
 output: step_13_b
// redemption phase is completed

// -- THE CLEARING PHASE -- //

user: RETAILER (R)   //STEP 14
 equation: step_14_a=concatenate(Cid,signWithKR (step_11_a,KRr), step_13_b);
 equation: step_14_b = encWithKU (step_14_a, KUf);
 output: step_14_b

user: MANIFACTURER (F)   //STEP 15
 equation: decWithKR (step_14_b, KRf);
// By using Cid F finds the User's (U) m-coupon data from its database
 equation: encDecWithKey (step_13_b, Kfu);
 equation: if (Nfu' == Nfu) {continue} else {abort MCWCC};  //The stored Nfu
          // value and the sent value by R are compared
 equation: if (O' == O) {continue} else {abort MCWCC};  //The stored O value
          // and the sent value by R are compared
 equation: step_15_a = hash (concatenate (O', MUC));  // hash value is
       // recalculated by using the stored MUC value and received O' value
 equation: if (step_15_a == step_11_a) {give the discount to R and continue}
            else {abort MCWCC};
            //Calculated hash value and received hash value are controlled

    //STEP 16
 equation: step_16 = encWithKU (signWithKR (Cid, KRf), KUp);
 output: step_16

user: COUPON_PROVIDER (P)
 equation: decWithKR (step_16, KRp);
 equation: store Cid as used m-coupon
```

KİŞİSEL YAYIN VE ESERLER

Yıldırım K., Demiray H. E., Simetrik ve asimetrik şifreleme yöntemlerine metotlar: Çırpılmış ve birleşik AKM-VKM, *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2008, **23**(3), 539-548.

Yıldırım K., Dalkılıç G., Duru N., Formally analyzed m-coupon protocol with confirmation code (MCWCC), *Turkish Journal Of Electrical Engineering & Computer Sciences*, 2019, **27**(1), 484-498.

Yıldırım K., Dalkılıç G., Duru N., Hsiang m-kupon protokolünün güvenlik analizi, *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 2018, (Kabul edildi).

ÖZGEÇMİŞ

Kerim Yıldırım 1976'da Balıkesir'de doğdu. İlk, orta ve lise öğrenimini Balıkesir'de tamamladı. Marmara Üniversitesi Elektronik ve Bilgisayar Öğretmenliği Bölümü'nden 1998 yılında mezun oldu. 2006 yılında Kocaeli Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimini tamamladı. Veri ve algoritma/protokol güvenliği alanlarında çalışmaları bulunmaktadır.