Journal of the Faculty of Engineering and Architecture of Gazi University 34:4 (2019) 1705-1724

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Security analysis of Hsiang m-coupon protocol

Kerim Yıldırım[1*], Gökhan Dalkılıç[2], Nevcihan Duru[1]
[1]Department of Computer Engineering, Kocaeli University, Kocaeli, 41380, Turkey
[2]Department of Computer Engineering, Dokuz Eylul University, İzmir, 35160, Turkey

Highlights:

- To show that the protocol is secure by the result of the security analysis obtained with the developed simulation and formal security analysis tool Scyther
- Examination of the protocol against known attacks by using man in the middle and eavesdropping
- Providing data security to seller and customer while shopping

Keywords:

- NFC
- M-coupon
- Security analysis
- Eavesdropping
- Scyther

Article Info:

Research Article
Received: 04.01.2018
Accepted: 28.12.2018

DOI:

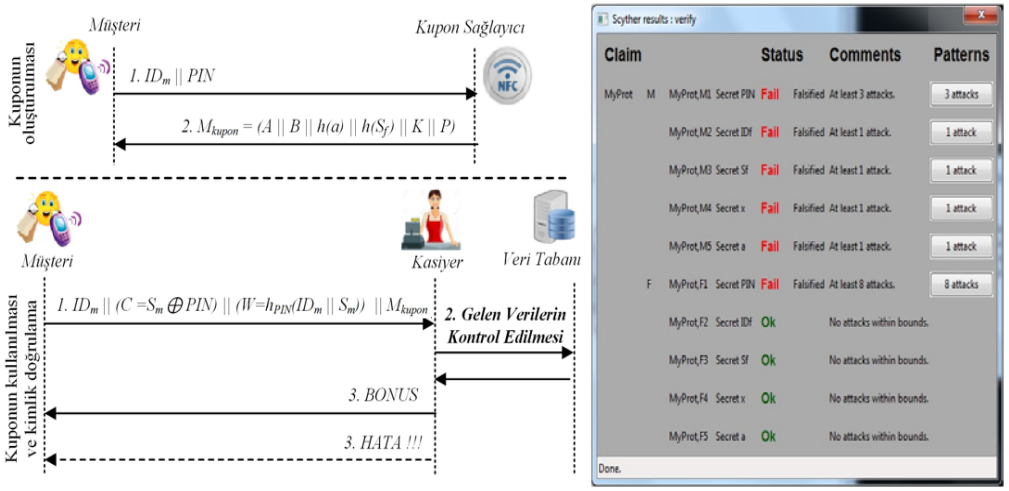
10.17341/gazimmfd.571490

Correspondence:

Author: Kerim Yıldırım
e-mail: kerim_yildirim@yahoo.com
phone: +90 262 303 3560

Graphical/Tabular Abstract

Although there are a large number of applications developed for users and their numbers increase day by day, the security analyzes of the applications do not progress in parallel with this increase. In the studies, the security analysis is never mentioned or is only described as superficial. 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.



(a) Hsiang's m-coupon protocol

(b) Analysis result of the protocol with the Scyther tool

Figure A. Security analysis of Hsiang's m-coupon protocol

Purpose: M-coupon scheme can't be secured just using only known cryptographic algorithms. Although cryptographic algorithms are an essential part of the protocol, security cannot be guaranteed by using cryptographic algorithms alone. Additionally security analysis of the protocol which is the essential part of the process must be done thoroughly. The fact that there is not enough work in this area and that there is often no explanation for the method by which security analyzes are claimed to be safe were the source of inspiration for this study. As a subject, the safety analysis of NFC-based m-coupons, which are considered to be widely used in the near future, has been selected.

Theory and Methods: Hsiang's NFC based m-coupon scheme has been analyzed by using Game Theory and automated security protocol validation tool Scyther. In the simulation, a communication is established between the coupon provider, the customer and the cashier, and the packages are sent. By listening the established communication, the attacker 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.

Results: At the issuing phase of Hsiang's m-coupon protocol some vulnerabilities have been found with the simulation and Scyther security analysis tool which is used to verify security protocols.

Conclusion: By using the vulnerabilities, some attacks have been illustrated to the scheme and then solutions are offered to these vulnerabilities.

Journal of the Faculty of Engineering and Architecture of Gazi University 34:4 (2019) 1705-1724

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Hsiang m-kupon protokolünün güvenlik analizi

Kerim Yıldırım[1]*, Gökhan Dalkılıç[2], Nevcihan Duru[1]
[1]Kocaeli Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kocaeli, 41380, Türkiye
[2]Dokuz Eylül Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İzmir, 35160, Türkiye

ÖNEÇIKANLAR

- Geliştirilen simülasyon ve otomatik güvenlik protokolü doğrulama aracı Scyther ile elde edilen güvenlik analizi sonucunda protokolün güvenli olduğunun gösterilmesi
- Protokolün ortadaki adam ve gizlice dinleme saldırıları ile çok bilinen ataklara dayanıklı olması
- Alışveriş yaparken satıcı ve müşteri verilerinin güvenliğinin sağlanması

Makale Bilgileri
Araştırma Makalesi
Geliş: 04.01.2018
Kabul: 28.12.2018

DOI:
10.17341/gazimmfd.571490

Anahtar Kelimeler:
NFC, m-kupon, güvenlik analizi, gizlice dinleme, Scyther

ÖZET

Günümüzde mobil cihazlar üzerlerinde barındırdıkları teknolojiler sayesinde günlük hayatın her alanına girmiştir. Bu uygulamalara örnek olarak yeni bir alan olan ve mobil cihazlarda kullanılan m-kupon uygulaması verilebilir. Mobil kupon kullanımının yaygınlaştırılabilmesi için gerekli olan hususlardan birisi, kullanıcı güvenliğinin sağlanmasıdır. M-kuponun elde edilmesi/kullanılması aşamasındaki güvenlik, sadece bilinen şifreleme algoritmaları kullanılarak sağlanamaz. Şifreleme algoritmaları protokolün olmazsa olmaz bir unsuru olmasına rağmen sadece şifreleme algoritmaları kullanılarak güvenlik garanti altına alınamaz. Bunlara ek olarak sürecin önemli bir parçası olan protokolün de güvenlik analizinin yapılması gerekmektedir. Bu kapsamda bu çalışmada, firmaların özel müşterilerine sağladığı özel indirimlerin müşterilere ulaştırılabilmesi için kullanılan m-kupon protokollerinden, Hsiang tarafından geliştirilen NFC tabanlı protokolün güvenlik analizi, oyun kuramı ve otomatik güvenlik protokolü doğrulama aracı Scyther kullanılarak yapılmıştır. Protokolün doğal elemanları olan kupon sağlayıcı, müşteri ve kasiyer için birer oyuncu ve saldırgan için ayrı bir oyuncu olmak üzere oyun kuramı için dört oyuncu belirlenmiştir. Bu amaçla senaryolar oluşturulmuş ve senaryoların simülasyonu yapılmıştır. Simülasyonda saldırganın, iletişimi dinleyerek elde ettiği paketleri çözüp çözemediği, sistemi manipüle edip edemediği incelenmiştir. İnceleme sonucunda, kuponun oluşturulması aşamasında, güvenlik zafiyeti olduğu, bu açık kullanılarak saldırılar yapılabildiği hem simülasyon ile hem de güvenlik protokollerinin doğrulanması amacıyla kullanılan Scyther aracı ile tespit edilmiş ve tespit edilen açıklar için çözüm önerileri sunulmuştur.

Security analysis of Hsiang m-coupon protocol

HIGHLIGHTS

- To show that the protocol is secure by the result of the security analysis obtained with the developed simulation and formal security analysis tool Scyther.
- Examination of the protocol against known attacks by using man in the middle and eavesdropping
- Providing data security to seller and customer while shopping

Article Info
Research Article
Received: 04.01.2018
Accepted: 28.12.2018

DOI:
10.17341/gazimmfd.571490

Keywords:
Micro tools, tool point FRF, stability diagrams, tool vibrations

ABSTRACT

Nowadays with technological development mobile devices equipped with new technologies and became part of our lives. For instance, a novel issue used on mobile devices: m-coupon. One of the important things that m-coupon usage needs to be widespread is ensuring of user security. M-coupon scheme can't be secured just using cryptographic algorithms. Although cryptographic algorithms are essential parts of the protocol, security cannot be guaranteed by using cryptographic algorithms alone. Additionally security analysis of the protocol must be done thoroughly. In this context, Hsiang's NFC based m-coupon scheme has been analyzed by using Game Theory and automated security protocol validation tool Scyther. Four players have been identified for Game Theory; an attacker added as a player to the protocol's natural players. In simulation, a communication is established between coupon provider, customer and cashier, and packages are sent. Attacker, by listening the established communication, examined whether he can unpack the packages he obtained or can manipulate the system. As a result, some vulnerabilities have been found at issuing phase with the simulation and Scyther security analysis tool. By using these vulnerabilities, some attacks have been illustrated to the scheme and then solutions are offered to these vulnerabilities.

*Sorumlu Yazar/Corresponding Author: kerim_yildirim@yahoo.com, dalkilic@cs.deu.edu.tr, nduru@kocaeli.edu.tr / Tel: +90 263 303 3560

1. GİRİŞ (INTRODUCTION)

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 [1], kullanıcının sağlık bilgilerini takip etme [2] 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 [3], mobil sensörler aracılığıyla kan basıncı, kan şekerinin ölçülmesi [3], üç eksenli akselerometre sensörü kullanılarak kullanıcının yürüdüğünün, koştuğunun, oturduğunun, merdiven tırmandığının anlaşılması [4], özellikle yaşlı ve bakıma muhtaç insanların düştüğü zaman kullanabilecekleri düşme analizi uygulamaları [5] 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 [6] standardında tanımlandığı şekilde 13,56 MHz frekansında çalışmaktadır. NFC teknolojisi kullanılarak mobil cihazlar için geliştirilen uygulamalara; cep telefonlarının banka kartı gibi kullanılması [7, 8], toplu taşımada bilet uygulaması [9, 11], turizm sektöründe bilet olarak kullanılması [12] sayılabilir.

NFC özellikli cep telefonlarının kullanımı yaygınlaştıkça bu özellik kullanılarak geliştirilen protokol/uygulamaların da sayısı artmaktadır. Bu uygulamalara örnek olarak hala gelişim sürecinde olan ve mobil cihazlarda kullanılmaya başlanan m-kupon uygulaması verilebilir. 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) [13] şansını yakalamaktadırlar. M-kuponlar müşterilere kısa mesajla (SMS), İnternet üzerinden, konum tabanlı servislerle ve gazete, dergi, broşürlere eklenmiş radyo frekansı ile tanımlama (radio frequency identification - RFID) özellikli posterler aracılığı ile ulaştırılabilmektedir [14].

M-kuponlar, firmalar tarafından özel müşterilerine özel indirimler vermek amacıyla da kullanılmakta, bu amaçla m-kupon protokolleri/uygulamaları geliştirilmektedir [14, 22]. 2007 yılında Dominikus ve Aigner tarafından NFC tabanlı bir m-kupon protokolü [15], 2008 yılında Hsiang vd. tarafından özet tabanlı (hash-based) NFC m-kupon protokolü [16], 2009 yılında Hsiang ve Shih tarafından özet tabanlı NFC m-kupon protokolünden [16] esinlenerek geliştirilen QR (quadratic residue theorem) tabanlı NFC m-kupon protokolü [17], 2010 yılında Hsueh ve Chen tarafından ağızdan ağıza/kulaktan kulağa yöntemi (word-of mouth - WOM) kullanılarak bir m-kupon paylaşım yöntemi önerilmiştir [14]. Önerilen protokol [14], 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 protokol [18], 2014 yılında Hsiang tarafından NFC tabanlı m-kupon protokolü [19] geliştirilmiştir. Chen vd. tarafından 2016 yılında güvenlik için açık anahtarlı şifreleme sistemi kullanılan NFC tabanlı bir m-kupon protokolü geliştirilmiş [20] ve 2016 yılında Yim tarafından, yine 2016 yılında Jiang vd. tarafından yeni protokoller önerilmiş ve bu m-kupon protokollerinin uygulamaları yapılmıştır [21, 22]. 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 [23]. Yapılan bu çalışmaların bir kısmında sadece protokol tanımlanırken [14, 19], diğer bir kısmı ise protokolün uygulamasını da içermektedir [20, 22]. Burada bahsedilen m-kupon protokollerinin yanı sıra m-kuponların kullanımına yönelik araştırmalar da bulunmaktadır [24].

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 [25]. Bu da alınması gereken güvenlik önlemlerinin ne kadar ciddi olduğunu gösteren bir örnektir.

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 protokollerin bile güvenlik analizlerinin hangi yöntemle yapıldığına yönelik bir açıklamanın çoğunlukla bulunmaması gerçeği, bu çalışmamızın esin kaynağı olmuştur. Konu olarak da, yakın gelecekte yaygın bir kullanım alanı bulacağı değerlendirilen NFC tabanlı m-kuponların güvenlik analizi seçilmiştir. Bu kapsamda m-kupon protokolleri içerisinden Hsiang tarafından geliştirilen m-kupon protokolü seçilmiş, protokolün JavaScript kullanılarak web tabanlı simülasyonu yapılmış ve oyun kuramı yöntemi ile analizi yapılmıştır. Ayrıca protokol, güvenlik protokollerinin doğrulanması için kullanılan Scyther aracı kullanılarak da analiz edilmiş,

ardından önerilen çözümlerin başarılı olup olmadığı yine Scyther ile kontrol edilmiştir.

Makalenin ikinci bölümünde bu çalışmada güvenlik analizini yaptığımız Hsiang protokolü anlatılmış, üçüncü bölümde protokolün analizi simülasyon üzerinden oyun kuramı kullanılarak yapılmış, daha sonra da otomatik güvenlik protokolü doğrulama aracı Scyther kullanılarak hem protokolün hem de açıkların giderilmesi için önerilen protokolün güvenlik analizi anlatılmış, dördüncü bölümde tartışma ve beşinci bölümde sonuçlara yer verilmiştir.

2. MATERYAL VE METOT (MATERIAL AND METHOD)

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

Bunlara ek olarak NFC Teknik Kılavuzunda [26] m-kupon algoritmalarının, ortadaki adam, kimliğine bürünme, yeniden gönderme, gizlice dinleme, yetkisiz kupon çoğaltımı/üretimi, çoklu kupon kullanımı 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 yapılmasının, sonrasında kullanıma sunulmasının, hem müşteriler hem de firmalar açısından hayati derecede önemli olduğu ortaya çıkmaktadır. Örneğin 2016 yılında Yim tarafından geliştirilen kupon sisteminin [21] güvenlik analizinin nasıl yapıldığı sunulan çalışmada belirtilmemiş, 2017 yılında Jiang vd. tarafından geliştirilen m-kupon dağıtımı modelinin [22] saldırılara karşı güvenlik analizinin gelecek çalışmalar kapsamında yapılacağı belirtilmiş, 2016 yılında Bartoli ve Medyet tarafından geliştirilen protokolde [23] 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.

Protokollerin güvenlik analizlerini yapmak için yöntem olarak oyun kuramı, simülasyonlar veya güvenlik protokolleri analiz araçları (CASPER/FDR, AVISPA, SCYTHER analiz araçları gibi) kullanılmaktadır. Örneğin Alshehri vd. tarafından, Dominikus ve Aigner'in birlikte geliştirdikleri protokolün [15] güvenlik analizi CASPER/FDR kullanılarak yapılmış, analiz sonucunda [27], 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 [28] Hsiang vd. tarafından geliştirilen özet tabanlı NFC m-kupon protokolünün [16] ve QR tabanlı NFC m-kupon protokolünün [17] güvenlik analizi CASPER/FDR kullanılarak yapılmıştır. Yapılan analiz sonucunda özet tabanlı protokolün 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 protokolü üzerinde yapılan analiz çalışmasında ise protokolün özet tabanlı protokole göre daha iyi olduğu ancak protokolde, kullanıcının kimlik doğrulama bilgilerinin doğru bir şekilde m-kuponuyla ilişkilendirilmediği bu nedenle de protokole kimlik doğrulama (User Authentication) saldırısının yapılabildiği belirtilmiştir [28].

Geliştirilen bu m-kupon protokollerinin güvenli oldukları ve saldırılara karşı dayanıklı oldukları iddia edilse bile protokolleri geliştirenlerle güvenlik analizini yapanlar aynı kişiler oldukları için yapılan testlerin yüzde yüz güvenilir olduğunu söylemek mümkün değildir. Alshehri vd. tarafından yapılan çalışma da [27], geliştirilen bir algoritma/protokolün güvenlik analizinin bağımsız kişi/kurumlarca da yapılmasının önemini ve güvenlik analizleri yapılmadan kullanılmaması gerektiğini bir kez daha göstermiştir.

NFC tabanlı olarak geliştirilen mobil uygulamalara/protokollere yönelik olarak güvenlik konusunda yapılan çalışmalara örnek olarak yatan hastalara verilen ilaçların NFC teknolojisi ile güvenli bir şekilde takip edilmesi [29] verilebilir. NFC'nin güvenliği ile ilgili 2006 yılında Haselsteiner ve Breitfuß tarafından [30], 2007 yılında Dominikus vd. tarafından [15] olası saldırılar hakkında çalışmalar yayınlamıştır. Ancak, her ne kadar m-kuponların uygulanabilirliği ve performans analizine yönelik çalışmalar [31] olsa da, güvenlik analizi yapılan bu çalışmalar ve m-kupon protokolleri incelendiğinde, m-kupon protokollerinin güvenlik analizine yönelik olarak sadece Alshehri vd. tarafından yapılan çalışmaların [27, 28] olduğu tespit edilmiştir.

Bu kapsamda NFC tabanlı uygulamaların yakın bir gelecekte yaygın olarak kullanılacağı değerlendirilmiş ve m-kupon protokollerinin güvenlik analizinin yapılmasına karar verilmiştir. Yapılan bu çalışmada m-kupon protokolleri içerisinden güncel olan protokollerden Hsiang tarafından geliştirilen NFC tabanlı m-kupon protokolü [19] seçilmiş ve güvenlik analizi yapılmıştır. Hsiang'ın tek başına ve/veya arkadaşları ile birlikte geliştirdiği m-kupon protokolleri [16, 17, 19] arasında yer alan bu protokol [19] 2014 yılında Hsiang tarafından tek başına yapılmış bir çalışmadır. Bu protokol 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 dağıtması), firmaların kendi dinamikleri ile sistemi idame edebilmelerine olanak tanıması ve yaptığımız araştırmalarda bu protokolün güvenlik açıklarına değinen bir çalışmanın olmaması nedenleriyle seçilmiştir. Hsiang tarafından geliştirilen m-kupon protokolünün [19], güvenlik analizi için Oyun Kuramının Sıfır Toplamı Modeli (kazan ya da kaybet) [32] kullanılmış ve bu amaçla simülasyon geliştirilmiştir. Simülasyon web (HTML) tabanlı olarak JavaScript kullanılarak tasarlanmış, protokolün 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 protokolün 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 protokolün güvenli olduğu sonucuna ulaşılmıştır.

Ayrıca oyun kuramı ve simülasyonla analiz yöntemine ilave olarak protokollerin güvenlik analizi için protokol güvenlik analiz araçlarından Scyther [33] kullanılarak hem protokolün 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.

2.1. Hsiang M-kupon Protokolü (Hsiang M-Coupon Protocol)

Hsiang tarafından yapılan çalışmada [19] önerilen protokolün 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. (Şekil 1)

Hsiang, önermiş olduğu protokolün yukarıda bahsedilen saldırılara karşı güvenli olduğunu belirtmektedir. Önerilen protokolde 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. Protokolde 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. Protokol iki aşamadan oluşmaktadır: kuponun oluşturulması, kuponun kullanılması ve kimlik doğrulaması.

2.1.1. Kuponun Oluşturulması Safhası (Issuing Phase)

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 Eş. 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 (Eş. 2). Aslında burada Eş. 1 ve Eş. 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 (Eş. 3 ve Eş. 4). Müşteriye M_{kupon} bilgisini göndermeden önce rasgele sayı S_f ve Eş. 1 ile elde etmiş olduğu a değerlerini kullanarak K değerini hesaplar (Eş. 5) ve hesapladığı değerleri müşteriye gönderir (Eş. 6). Kuponun oluşturulması işlemleri Şekil 1'de ve kullanılan sembollerin anlamları semboller başlığı altında gösterilmiştir.

$$a = h(ID_f) \oplus S_f \oplus ID_m \tag{1}$$

$$P = S_f \oplus x \oplus PIN \tag{2}$$

$$A = a^2 mod\ n \tag{3}$$

$$B = S_f^2 mod\ n \tag{4}$$

$$K = h_{Vf}(S_f \| a) \tag{5}$$

$$M_{kupon} = (A \| B \| h(a) \| h(S_f) \| K \| P) \tag{6}$$

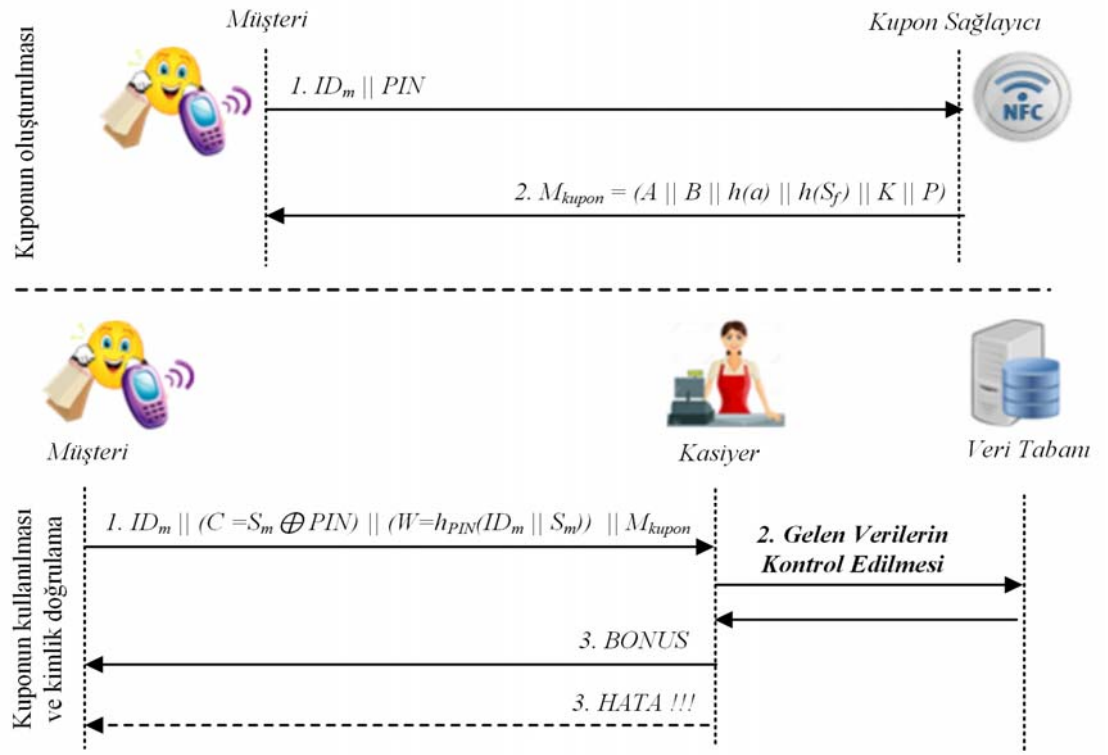
2.1.2. Kuponun Kullanılması ve Kimlik Doğrulama (Redemption and Authentication)

Müşteri m-kuponu kullanmak için, rasgele bir sayı (S_m) üretir. S_m ve ID_m değerlerini kullanarak Eş. 7 ve Eş. 8 ile C ve W değerlerini hesaplar. Bu değerler ile birlikte ID_m ve Eş. 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 9-12 numaralı eşitlikleri kullanarak W' değerini hesaplar. Hesapladığı W' değeri ile W değerini karşılaştırır. Eğer değerler farklı ise kupon reddedilir.

$$C = S_m \oplus PIN \tag{7}$$

$$W = h_{PIN}(ID_m \,||\, S_m) \quad (8)$$

$$S_f = h(ID_f) \oplus ID_m \oplus a \quad (9)$$



Şekil 1. Hsiang m-kupon protokolü [19] (Hsiang's m-coupon protocol)

$$PIN = P \oplus S_f \oplus x \quad (10)$$

$$S_m = C \oplus PIN \quad (11)$$

$$W' = h_{PIN}(ID_m \,||\, S_m) \quad (12)$$

$$h(ID_f) = a \oplus S_f \oplus ID_m \quad (13)$$

$$V_f' = h_x(ID_f \,||\, Teklif) \quad (14)$$

$$K' = h_{Vf}'(S_f \,||\, a) \quad (15)$$

Kasiyer, Eş. 3 ve Eş. 4 ile yapılan açık anahtarlı şifreleme işlemini çözmek için Çin artık teoremini (Chinese remainder theorem) [34] 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 (Eş. 9). Elde ettiği S_f değerini kullanarak müşterinin PIN değerini elde eder (Eş. 10) ve müşterinin üretmiş olduğu S_m değerini Eş. 11 ile hesaplar. Kasiyer gelen verilerden elde etmiş olduğu değerleri kullanarak W' değerini hesaplar (Eş. 12). Hesapladığı W' değeri ile müşterinin göndermiş oluğu W değeri aynı ise kasiyer $h(ID_f)$ değerini elde etmek için Eş. 13'ü kullanır. Kasiyer elde ettiği $h(ID_f)$ değerini kullanarak veri tabanından kupon sağlayıcının (ID_f) verdiği kupon bilgilerini (*Teklif*) bulur. Sonrasında 14 ve 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 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 protokolde, 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 $A = a^2 mod\ n$ eşitliğinde kullanılan a değerinin p, q ve n değerleri bilinmeden bulunabilmesinin matematiksel olarak mümkün olmadığı, protokolün yeniden gönderme saldırısı (replay attack), kupon kopyalama/çoğaltma, kuponun çoklu kullanımı, yetkisiz kupon üretme ve veri değiştirme ataklarına karşı dayanıklı olduğu belirtilmiştir.

Burada $A = a^2 mod\ n$ 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 protokolde 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 [35].

3. SONUÇLAR (RESULTS)

Güvenlik analizi için protokole, 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 protokolün güçlü kısımları, ikinci kısımda ise güvenlik açıkları gösterilmiştir.

3.1. Protokolün Güçlü Kısımları (Strong Parts of the Protocol)

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

3.1.1. Ortadaki adam saldırısı (Man-in-the-middle attack)

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 protokolün 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.

3.1.2. Kuponların çoklu kullanımı saldırısı (Multiple cash-in attack)

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 Eş. 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.

3.1.3. Yeniden gönderme saldırısı (Replay attack)

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. Protokolün Zayıf Kısımları (Weak Parts of the Protocol)

Tüm sürecin firmanın kendisi tarafından yönetilmesi protokol 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 [36, 37] müşterilerin bu tarz siteleri kullanmayı tercih ettiklerini göstermektedir. Ayrıca, eğer firmanın birden fazla şubesi var ise bu protokolü 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. Protokole uygulanabilecek saldırı senaryoları aşağıda alt başlıklarda sunulmuştur.

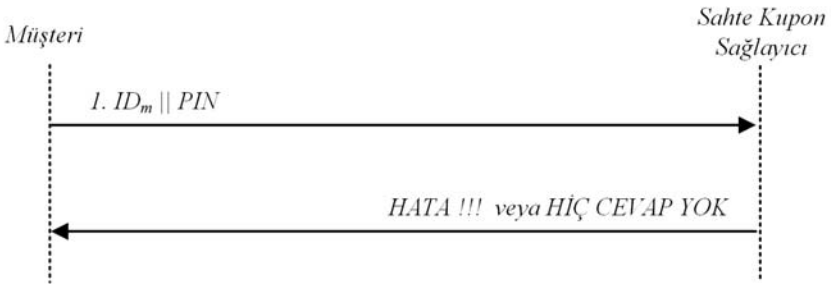
3.2.1. Müşterinin kimlik bilgilerinin çalınması (Impersonation attack)

Bu saldırı senaryosu müşterinin indirim kuponunu ilk alacağı/oluşturulacağı zamanı kapsamaktadır. Senaryoda saldırı sahte bir kupon sağlayıcı ile (Oltalama Saldırısı - Phishing) (Şekil 2) veya var olan bir kupon sağlayıcının önüne bir pasif NFC okuyucu konulması şeklinde (iletişimi

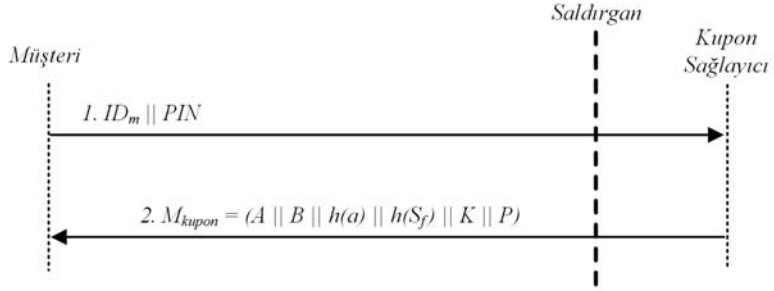
gizlice dinleme) (Şekil 3) planlanmıştır. Senaryoda firma, kuponların dağıtımını NFC özellikli posterler aracılığı ile yapmaktadır. Saldırgan fiziksel olarak aynı görünümlü bir poster üreterek müşterilerin ilgisini çekmeye çalışmakta veya çok basit olarak NFC okuyucu özelliği olan bir okuyucuyu posterin üzerine yapıştırıp müşterinin indirim kuponunu normal olarak almasını beklemektedir. Şekil 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'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. 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 (Şekil 4) ve sözde kodları Bölüm 3.2.1.1.'de verilmiştir.

3.2.1.1. Müşterinin bilgilerinin çalınması ve yetkisiz kupon kullanma/üretme saldırılarına ait simülasyonun akış diyagramı ve sözde kodları
(Flow chart and pseudo codes of the simulations of impersonation and unauthorized coupon copying/generation attacks)

```
// SİMÜLASYONUN SÖZDE KODLARI

// Müşterinin kimlik bilgilerinin çalınması (Impersonation attack)
// yetkisiz kupon kullanma (unauthorized coupon copying/generation) saldırılarının başlangıcı
// user: MUSTERI// Müşterinin yapmış olduğu işlemler
m_IDm = 1111;  // Müşterinin ID değeri
m_PIN = 1234;  // Müşterinin PIN değeri
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
s_IDm = m_IDm;          // Saldırgan müşteriden elde etmiş olduğu m_IDm= 1111 değerini
// kendi ID değeri olarak kullanıyor.
s_PIN = m_PIN;          // Saldırgan müşteriden elde etmiş olduğu m_PIN= 1234 değerini
// kendi PIN değeri olarak kullanıyor.
sendValue (s_IDm, s_PIN)  // Bu bilgiler saldırgan tarafından kupon sağlayıcıya gönderiliyor.
// Amaç yeni bir m-kupon elde etmek
// Müşterinin kimlik bilgilerinin çalınması saldırısının sonu (Impersonation attack)

// user: KUPON_SAĞLAYICI    // Kupon sağlayıcının yapmış olduğu işlemler
receive_IDm = s_IDm;    // Saldırgandan gelen bilgiler
receive_PIN = s_PIN;    // Saldırgandan gelen bilgiler
IDm = 1111;     // Kupon sağlayıcının veri tabanında kayıtlı olan müşterinin ID değeri
PIN = 1234;     // Kupon sağlayıcının veri tabanında kayıtlı olan müşterinin PIN değeri
```



Şekil 2. Kuponun elde edilmesi aşamasında oltalama saldırısı (Phishing attack at issuing phase)



Şekil 3. Kuponun elde edilmesi aşamasında iletişimi dinleme (Eavesdropping at issuing phase)

```
IDf= 2222;          // Kupon sağlayıcının ID değeri
Sf= 6543;           // Kupon sağlayıcının kupon için üretmiş olduğu rasgele sayı
x= 9876;            // Kupon sağlayıcının kurum için haberleşmede kullanmış olduğu gizli anahtar
teklif= 25;         // Kuponun indirim oranı
if (IDm == receive_IDm && PIN == receive_PIN) {alert ("MUSTERI ONAYLANDI")}
  else {alert ("Uzgunum!!! MUSTERI GECERLI DEGIL.");
 throw new Error('Uygulama sonlandırıldı !!!') }
a = xorData(xorData (hash(IDf), Sf), IDm) // a değeri hesaplanıyor
P = xorData(xorData(Sf, x), PIN)  // P değeri hesaplanıyor
A = calculateA(a)                 // A değeri hesaplanıyor
B = calculateB(Sf)                // B değeri hesaplanıyor
// 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 = hashWithKey (IDf, teklif, x)  // Vf değeri hesaplanıyor
K = hashWithKey (Sf, a, Vf)        // K değeri hesaplanıyor
a_hash = hash (a)                  // a_hash değeri hesaplanıyor
sf_hash = hash (Sf)                // sf_hash değeri hesaplanıyor
sendValue (A, B, a_hash, sf_hash, K, P)  // M-kupon bilgisi farkında olmadan
// doğrudan saldırgana gönderiliyor

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

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

Sf = xorData(xorData (hash(IDf), receive_IDm), a)  // Sf değerini hesaplıyor

PIN = xorData(xorData(P, Sf), x)   // PIN değerini hesaplıyor
s_Sm = xorData(receive_C, PIN)     // s_Sm değerini hesaplıyor
Ww = hashWithKey (receive_IDm, s_Sm, PIN)  // Ww değerini hesaplıyor
if (W = Ww) { alert ("DEGERLER AYNI")}     // Elde edilen değerler karşılaştırılıyor
else {alert ("Uzgunum!!! KUPON GECERLI DEGIL.");
throw new Error(' Uygulama sonlandırıldı !!!') }
hIDfValue = xorData(xorData(a, Sf), receive_IDm)  // hIDfValue değerini hesaplıyor
Vff = hashWithKey (IDf, teklif, x)  // Vff değerini hesaplıyor
Kk = hashWithKey (Sf, a, Vff)       // Kk değerini hesaplıyor
if (K = Kk) {alert ("KUPON GECERLI, INDIRIM UYGULANDI")}  // Elde edilen değerler
else {alert ("Uzgunum!!! KUPON GECERLI DEGIL."); // karşılaştırılıyor
 throw new Error(' Uygulama sonlandırıldı !!!')}  // Bu aşamaya kadar sorun yoksa kasiyer indirimi uyguluyor.
// Yetkisiz kupon kullanma/üretme saldırısının sonu (unauthorized coupon copying/generation)
```

3.2.2. Yetkisiz kupon kullanma/üretme
(Unauthorized coupon copying/generation)

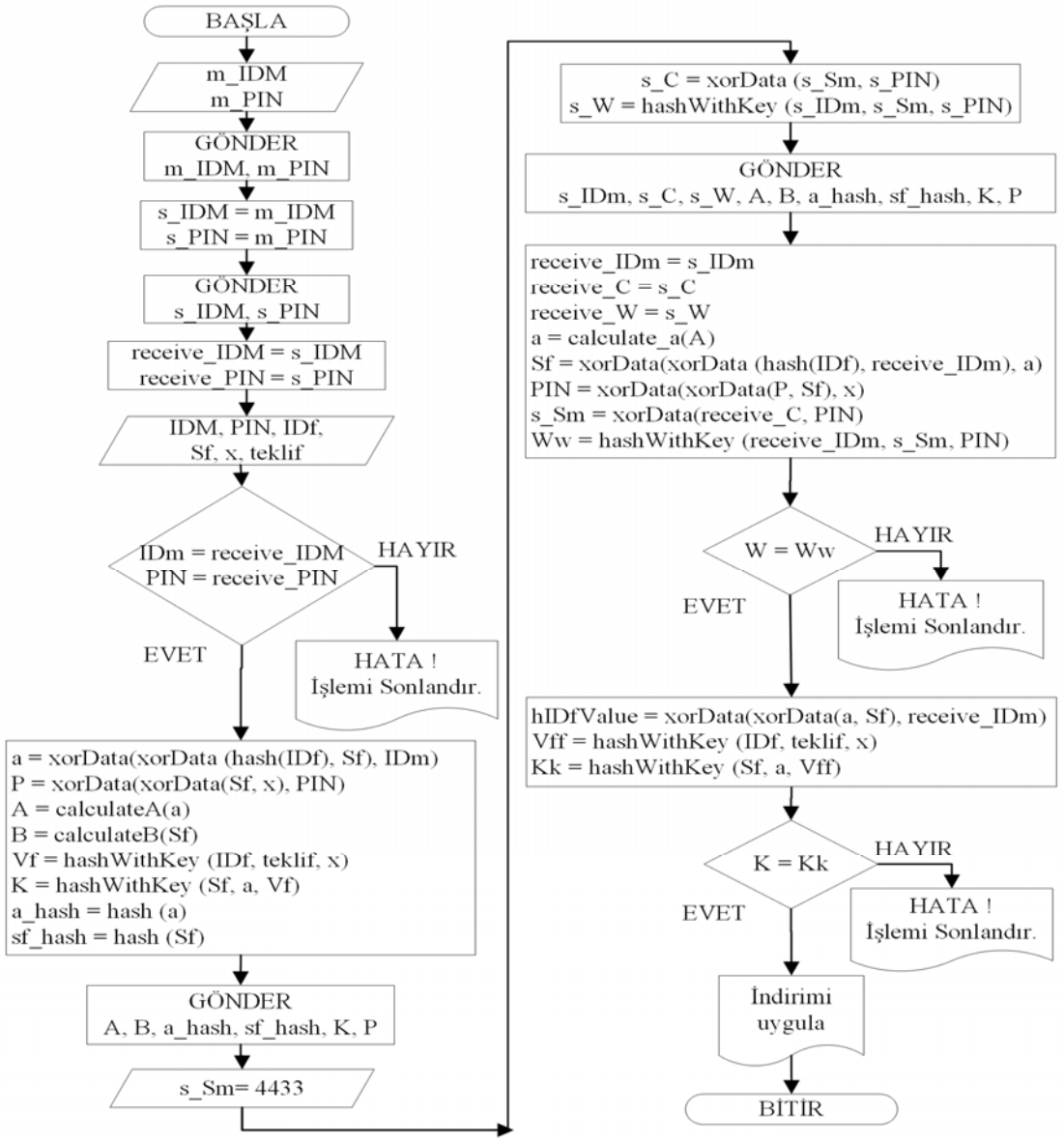
ID_m ve *PIN* değerlerini elde eden saldırgan, gerçek müşterinin yerine geçme ve geçerli bir kupon elde etme şansına sahip olmuştur. Bu saldırı özellikle özel müşterilere özel olarak tanımlanan indirimlerin kullandırılmasında soruna neden olur. Örneğin, sürekli alışveriş yapan müşterilere belirli bir 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 5'te gösterilen saldırı şu adımlardan oluşmaktadır:

- Saldırgan ilk olarak kuponun oluşturulması aşamasında müşterinin ID_m ve *PIN* değerlerini oltalama saldırısı ile elde eder (Şekil 5 birinci kısım).
- Elde ettiği bu değerleri kullanarak normal bir müşteri gibi kupon sağlayıcıdan yeni bir m-kupon talep eder ve alır (Şekil 5 ikinci kısım).
- Daha sonra elde ettiği kuponu kullanmak için kasiyere götürür ve istemiş olduğu indirimi gerçek müşterinin yerine alır (Şekil 5 üçüncü kısım). Saldırı için yapılan simülasyonun akış diyagramı ve sözde kodları Bölüm 3.2.1.1.'de verilmiştir.

3.2.3. Kuponun geçersiz hale getirilmesi saldırısı
(Invalidation of the coupon attack)

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



Şekil 4. Simülasyonun akış diyagramı (Flow chart of the simulation)

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;

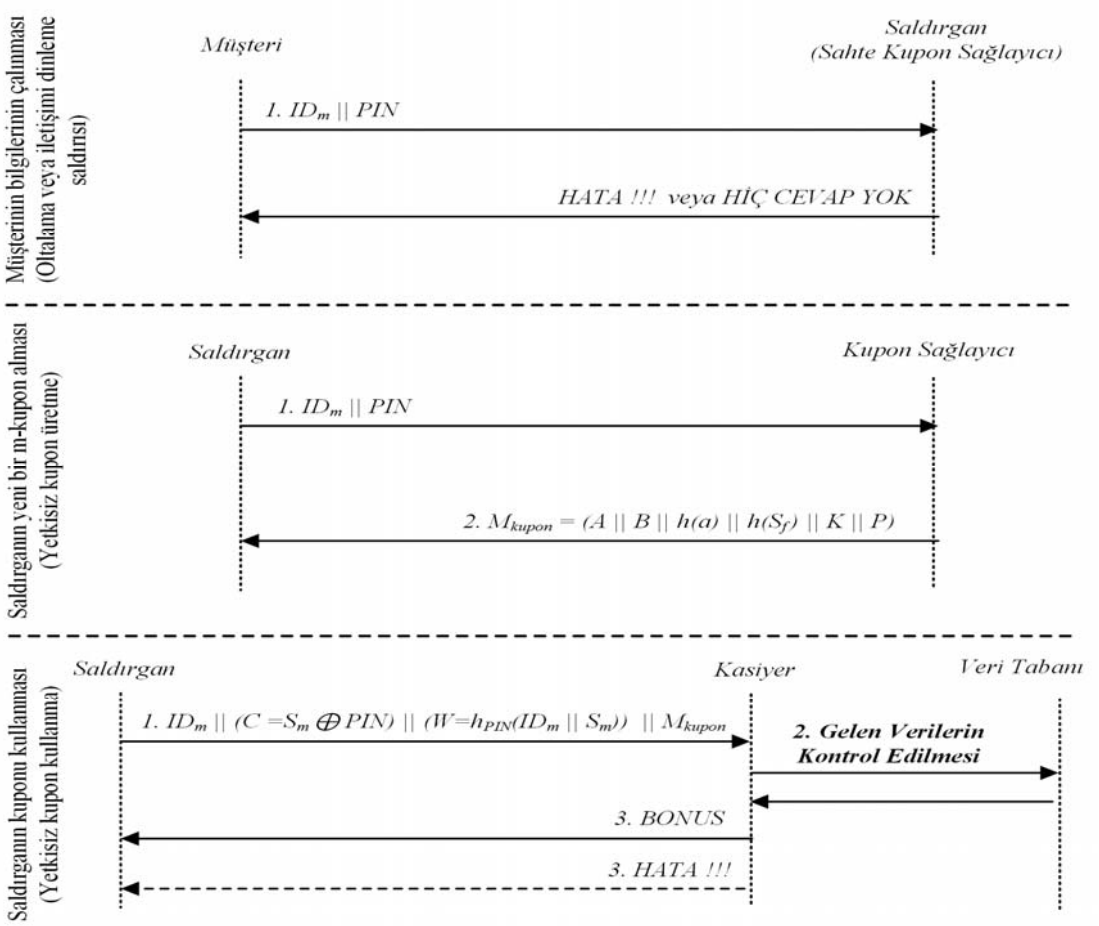
Saldırgan müşterinin kimlik bilgilerini kullanarak kendisine yeni kuponlar oluşturmak yerine firmanın doğrudan imajına ve güvenirliliğine zarar vermek için farklı bir yöntem izleyebilir. Saldırgan, müşterinin almış olduğu kuponu geçersiz hale getirebilir. Şekil 6'da gösterilen saldırı şu adımlardan oluşmaktadır:

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.

Müşteri normal bir şekilde m-kuponunu elde eder.

Müşteri aldığı kuponu kullanmak üzere kasiyere giderken saldırgan devreye girer ve atak başlar.

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



Şekil 5. Saldırganın kuponu elde etmesi ve kullanması (Attacker gets and uses the coupon)

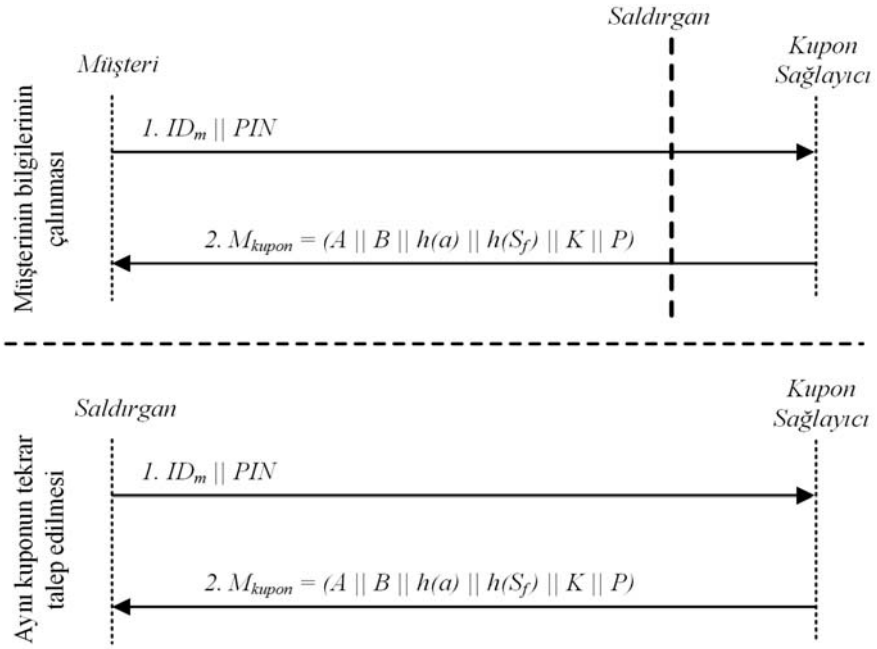
değişmiş olur. Böylece m-kupon yeniden üretilmiş ve eski m-kupon geçersiz hale gelmiş ve saldırı başarılı olmuştur. Hiçbir şeyden haberi olmayan müşteri kasiyere gidip kuponu kullanmak istediğinde kuponunun geçersiz olduğunu öğrenir ki bu istenilmeyen bir durumdur. Bu saldırı doğrudan firmanın güvenirliliğine 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.

3.2.4. Gizli anahtarın elde edilmesi saldırısı
(Secret disclosure attack)

Hsiang, önermiş olduğu protokolün yapılacak saldırılara karşı güvenli olduğunu, saldırganın istese de m-kupon bilgisini M_{kupon} = *(A || B || h(a) || h(S_f) || K || P)* çözemeyeceğini, Eş. 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 protokolün kupon sağlayıcının *ID*'sinin gizliliğini sağlayacağını iddia etmiştir. Ancak, yapmış olduğumuz çalışmada burada gözden kaçan bir nokta olduğunu tespit ettik. Protokol, 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:

- Saldırgan "Müşterinin Bilgilerinin Çalınması Saldırısı"nı gerçekleştirerek müşterinin ID_m ve *PIN* değerlerini elde eder.
- Ardından kupon sağlayıcıya giderek herhangi bir m-kupon talebinde bulunur.
- Kupon sağlayıcı saldırgana istemiş olduğu m-kuponu gönderir. Saldırgan kupon sağlayıcıdan gelen M_{kupon} bilgisini elde eder.
- 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.
- Saldırgan ID_m, *a* ve S_f değerlerini kullanarak Eş. 13 ile $h(ID_f)$ değerini elde eder.
- Sonrasında *PIN, P* ve S_f değerlerini kullanarak *x* değerini elde eder (Eş. 16). Protokolde de bahsedildiği gibi *x* değeri kupon sağlayıcı, kasiyer ve veri tabanı arasında kullanılan sabit gizli anahtardır, dolayısıyla saldırgan bu gizli anahtarı elde edebilmektedir.

$$x = P \oplus S_f \oplus PIN \tag{16}$$



Şekil 6. M-kuponun geçersiz hale getirilmesi (Invalidation of the m-coupon)

Tablo 1. Saldırı öncesi bilenen, saldırı sonrasında elde edilen değerler (Known values before and after attack)

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*

Eş. 16 ile yapılan işlemle saldırgan artık gizli anahtara da sahiptir. Elinde olmayan değerler ise kasiyer ile veri tabanı arasındaki iletişimde kullanıldığı belirtilen Eş. 14 ve Eş. 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 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 protokolde herhangi bir bilgi bulunmamaktadır.

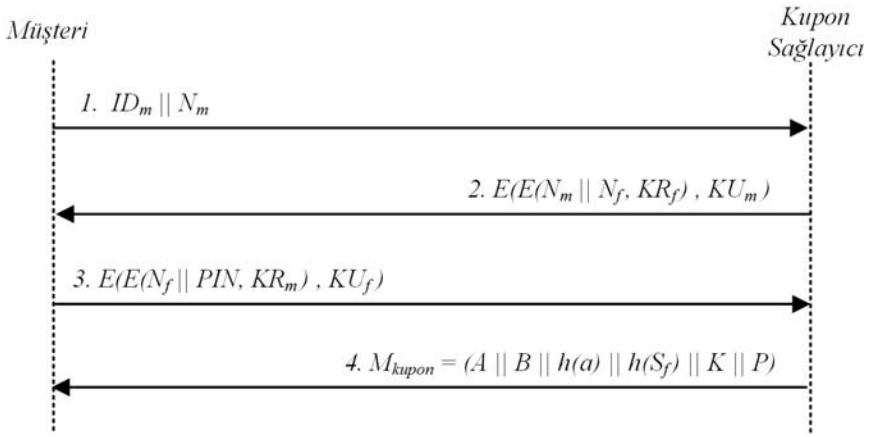
3.3. Saldırılara Sunulan Çözüm Önerileri
(Solution for the Attacks)

3.3.1. Müşterinin kimlik bilgilerinin çalınması, yetkisiz kupon kullanma/üretme ve kuponun geçersiz kılınması saldırılarına çözüm önerisi
(Solution for impersonation and unauthorized coupon copying/generation and invalidation of the coupon attacks)

Hsiang tarafından geliştirilen protokolde 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 [27], [38] protokolleri) veya karşılıklı kimlik kontrolüne ilave olarak müşterinin sahip olduğu fiziksel özellikleri de kontrol aşamasına ekleyen yöntemler de (müşterinin parmak izini kimlik kontrolü olarak kullanan protokol [39]) 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 protokolün düzenlenmiş hali Şekil 7'de sunulmuştur. İlk aşamada müşteri öncelikle kendi ID değerini (ID_m) ve rasgele üretmiş olduğu N_m değerini kupon



Şekil 7. Kuponun oluşturulması aşamasındaki açıklığın giderilmesi (Prevention of the vulnerability at the issuing phase)

sağlayıcıya gönderir (Eş. 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 ($E(N_m \| N_f, KR_f)$) ve göndermiş olduğu verilerin sadece müşteri tarafından açılmasını sağlamak için de imzaladığı veriyi müşterinin açık anahtarı ile şifreler (Eş. 18) ($E(E(N_m \| N_f, KR_f), KU_m)$). Müşteri Eş. 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 (Eş. 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.

$$ID_m \| N_m \tag{17}$$

$$E(E(N_m \| N_f, KR_f), KU_m) \tag{18}$$

$$E(E(N_f \| PIN, KR_m), KU_f) \tag{19}$$

3.3.2. Gizli anahtarın elde edilmesi saldırısına çözüm önerisi
(Solution for secret disclosure attack)

Protokolde, 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.

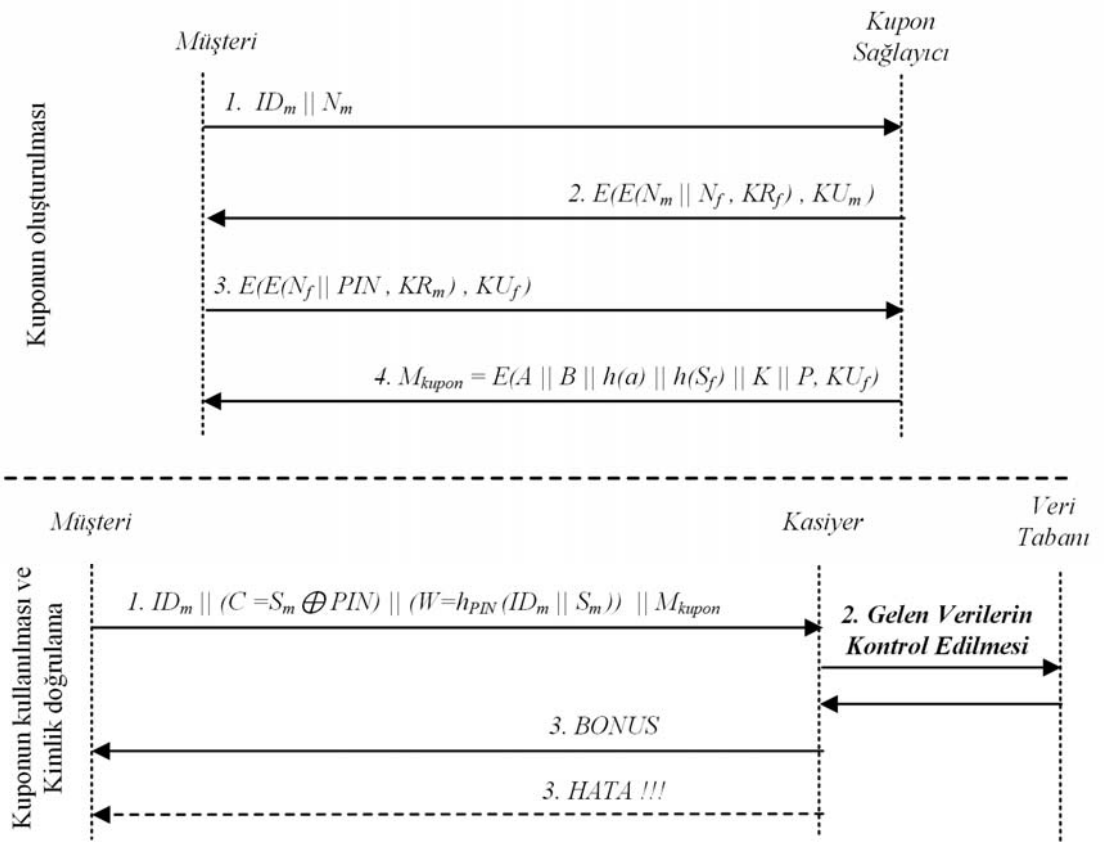
Gizli anahtarın elde edilmesi saldırısını önlemek için kupon oluşturulması aşamasında müşteriye gönderilen m-kupon verileri kupon sağlayıcının açık anahtarıyla şifrelenmelidir:

$$M_{kupon} = E(A \| B \| h(a) \| h(S_f) \| K \| P, KU_f) \tag{20}$$

Güvenliği sağlamak için, Eş. 20 ile ekstra yapılan açık anahtarlı şifreleme yöntemi süreci olumsuz olarak etkilemeyecektir. Çünkü şifreleme işlemi (Şekil 8'de kuponun oluşturulması aşamasındaki ikinci adım) ve şifrenin çözülmesi işlemi (Şekil 8'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 protokolün son hali Şekil 8'de gösterilmiştir.

3.4. Protokolün Güvenlik Analiz Aracı Scyther ile analizi
(Analysis of the Protocol with Formal Security Analysis Tool Scyther)

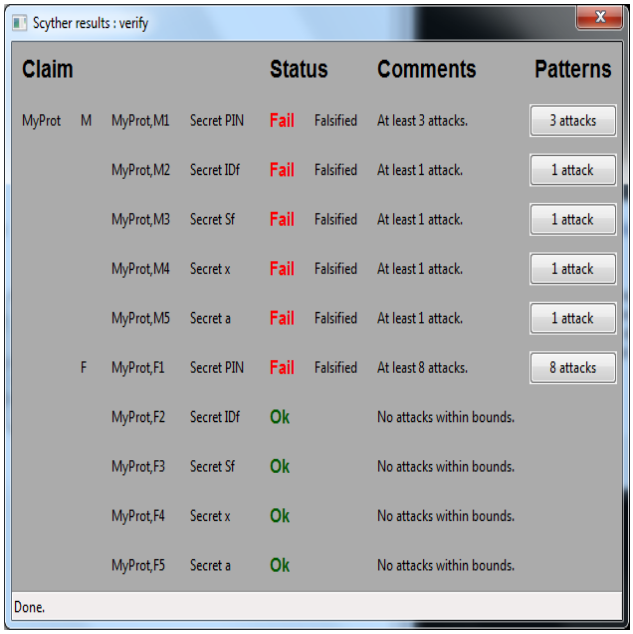
Scyther aracı tüm olası protokol davranışlarının sonlu bir sunumunu yaparak protokolleri karakterize edebilen güçlü bir güvenlik protokol analiz aracıdır. Bu araç, atakların, olası



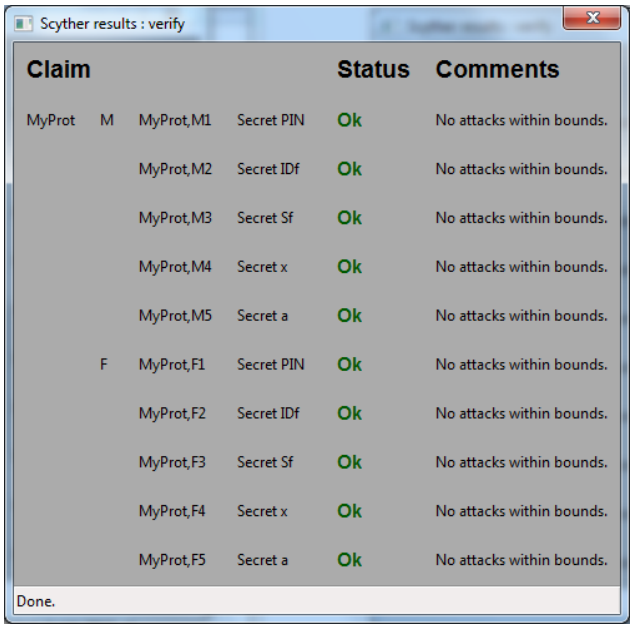
Şekil 8. Yeniden düzenlenen protokol (Revised protocol)

protokol davranışlarının ve protokollerin doğruluğunun kontrol edilmesini ve hataların tespit edilmesini sağlar [33]. Scyther aracı kullanılarak yapılan protokol analizleri arasında IKEv1 and IKEv2 protokolleri [40], ISO/IEC 11770 standardı [41], ISO/IEC 9798 standardı [42] sayılabilir. Scyther aracı kullanılarak yapılan onlarca protokol analizi bulunmaktadır. Bahse konu protokol analizlerine [43] ve diğer incelemelere ulaşmak için web sayfaları [44] ziyaret edilebilir. Hsiang protokolünü Scyther kılavuzuna [45] göre kodlarken protokolde 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 protokolde herhangi bir sayıda "*role*" olabilir ve protokolde 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, protokolde 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 protokolün analizi için Scyther v1.1.3 Windows sürümünü kullandık. Protokolde rolleri ve değişkenleri tanımladıktan sonra saldırgandan korunması gereken verileri belirledik ve korunması gereken verileri *claim* parametresi ile gösterdik. Protokolün, bu değerlerin güvenliğini/gizliliğini sağlaması gerekmektedir. Yapılan kodlama (Hsiang_protokolu.spdl) Bölüm 3.4.1'de verilmiştir. Analiz sonucunda Hsiang'ın protokolünün belirtildiği kadar güçlü olmadığı, protokolde açık olduğu, korunması gereken verilerin gizliliğini/güvenliğini sağlayamadığı ve bu açık kullanılarak saldırılar yapılabileceği Scyther aracı tarafından da teyit edilmiştir (Şekil 9). 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 safhasındaki açıktan kaynaklandığı görülmüştür. Şekil 9'da verilen analiz sonucunda da görüleceği üzere protokole yönelik toplamda 15 adet saldırı tespit edilmiş olup araç tarafından tespit edilen saldırılardan birisi Şekil 11'de gösterilmiştir. Yapılan bu saldırıda protokol 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 8'de

gösterilen önermiş olduğumuz protokolün, gerçekten bizim iddia ettiğimiz gibi gerekli güvenlik kriterlerini sağlayıp sağlamadığını kontrol etmek amacıyla, önerdiğimiz protokolü Scyther kılavuzuna [45] göre kodladık. Yapılan kodlama (Hsiang_protokolu_onerilen_hali.spdl) Bölüm 3.4.2'de verilmiştir. Yapılan analiz sonucunda önerilen yapının gerekli güvenliği sağladığı ve herhangi bir saldırının yapılamadığı tespit edilmiş ve analiz sonucu Şekil 10'da verilmiştir.



Şekil 9. Protokolün Scyther aracı ile yapılan analizinin sonucu (Analysis result of the protocol with the Scyther tool)

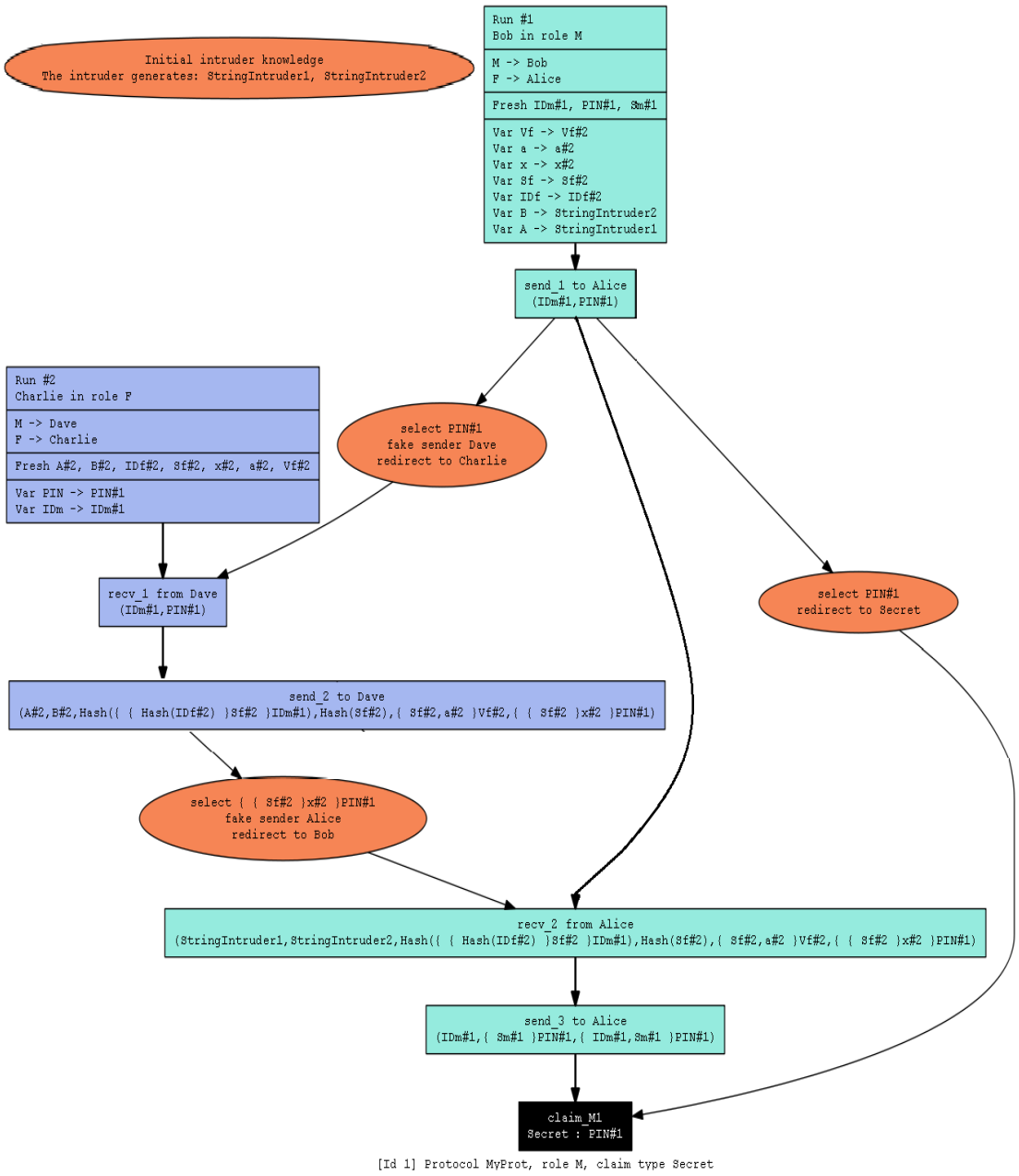


Şekil 10. Önerilen protokolün Scyther aracı ile yapılan analizinin sonucu
(Analysis result of the proposed protocol with the Scyther tool)

3.4.1. Hsiang tarafından geliştirilen protokolün Scyther aracı için yazılan kodları
(Hsiang's m-coupon protocol codes written for the Scyther tool)

Hsiang tarafından geliştirilen protokolün 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_protokolu.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);
 }
}
```



Şekil 11. Scyther aracı ile tespit edilen örnek bir saldırı (An example of attacks found by the Scyther tool)

3.4.2. Saldırılara karşı önerilen protokolün Scyther aracı için yazılan kodları
(The proposed m-coupon protocol codes written for the Scyther tool)

Hsiang tarafından geliştirilen protokole yönelik olarak yapılan saldırıları engellemek için önerilen protokolün 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_protokolu_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);
 }
}
```

4. SONUÇLAR VE TARTIŞMALAR (RESULTS AND DISCUSSIONS)

Veri güvenliği analizlerine yönelik olarak, Görmüş vd. tarafından nesnelerin İnterneti teknolojisinde güvenli iletişim için kullanılan protokoller, küçük cihazların mimari yapısı dikkate alınarak incelenmiş [46], Okkalıoğlu vd. tarafından gizlilik tabanlı ortak filtreleme sistemlerinin güvenliğinin analiz edilmesi için sisteme atakların yapıldığı ve gizli verinin elde edilip edilemediğinin kontrol edildiği bir çalışma [47] yapılmıştır.

Hem Alshehri vd. tarafından, Dominikus ve Aigner'in birlikte geliştirdiği protokolün [15] güvenlik analizi [27], hem Alshehri tarafından tez çalışması olarak yapılan [28] Hsiang vd. tarafından geliştirilen özet tabanlı NFC m-kupon protokolünün [16] ve QR tabanlı NFC m-kupon protokolünün [17] güvenlik analizleri, hem Görmüş vd. [46], hem Okkalıoğlu vd. yapmış olduğu çalışma [47], hem de yapılan bu çalışma göstermektedir ki, geliştirilen tüm algoritma ve protokollerin güvenlik analizlerinin tasarım aşamasında yapılması gerekmektedir. Burada asıl sorun, araştırmacılar tarafından geliştirilen protokollerin çok azında güvenlik analizi için kullanılan yöntemden bahsedilmesidir. Genellikle tasarımı yapanlar kendi yorumları doğrultusunda tasarımlarının güvenli olduğunu iddia etmektedirler. Bu nedenle de sistemin güvenilir olup olmadığının kontrolünün başka araştırmacılar tarafından yapılması gerekmektedir. Diğer taraftan da sistemlerin güvenlik kontrollerinin bağımsız kişilerce yapılmasının sisteme olan güveni olumlu yönde etkileyeceği de düşünülebilir. Güvenlik analizi konusunda yapılan çalışmalar ile birlikte bu çalışmanın yeni tasarlanacak olan sistemlere/protokollere, bakış, analiz ve inceleme yöntemi olarak rehberlik edeceği, araştırmacılara saldırı yöntemleri, saldırıların önlenmesi ve güvenlik analizi konusunda ışık tutacağı, var olan algoritmaların/protokollerin de güvenlik analizlerinin yapılmasına katkı sağlayacağı, ayrıca yapmış olduğumuz bu çalışmada analiz için birden fazla yöntemin (simülasyon, protokol güvenlik analiz aracı) kullanılmış olmasının da, protokollerin dizayn aşamasında tasarıma farklı bakış açılarından (hem güvenlik hem de uygulanabilirlik) bakılmasına ve protokollerin daha güvenilir olarak tasarlanmasına katkı sağlayacağı kanaatindeyiz.

5. SİMGELER (SYMBOLS)

$E(...)$	: Şifreleme algoritması
$h(...)$	: Kriptografik özet fonksiyonu
ID_f	: Kupon sağlayıcının ID'si
ID_m	: Müşterinin ID'si
KR_m	: Müşterinin gizli anahtarı
KU_f	: Kupon sağlayıcının açık anahtarı
M_{kupon}	: Müşteriye gönderilen m-kupon
PIN	: Müşteri kodu
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.)
Vf	: Kasiyer ve kupon sağlayıcılar arasında paylaşılan gizli anahtar
X	: Kupon sağlayıcı ve kasiyerin sabit gizli anahtarı

6. SONUÇLAR (CONCLUSIONS)

Yapılan bu çalışmada, protokollerin güvenlik analizi için kullanılan yöntemlerden olan Oyun Kuramı, simülasyon yöntemi ve otomatik güvenlik protokolü doğrulama aracı Scyther kullanılmıştır. Hsiang tarafından geliştirilen m-kupon protokolünün 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 protokolün güvenli olduğu anlaşılmıştır.

Bu çerçevede yapılan güvenlik analizi sonucunda; Hsiang tarafından, tüm güvenlik kontrollerinin m-kuponun

Tablo 2. Protokole yapılabilen saldırılar (Attacks to the protocol)

Saldırının Adı	Hsiang Protokolü	Önerilen Protokol
Yetkisiz kupon kullanma saldırısı	EVET	HAYIR
Yetkisiz kupon kopyalama/çoğaltma saldırısı	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

kullanılması safhasında yapıldığı, kuponların müşterilere ulaştırılması aşamasında (kuponun oluşturulması safhası) 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 kılınabileceği tespit edilmiştir.

Ayrıca Hsiang'ın iddia ettiği gibi protokolün, 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 protokolün (Şekil 8) istenilen güvenlik düzeyini karşıladığı görülmüştür.

Daha sonra Hsiang tarafından geliştirilen protokol, protokol 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. Protokolde tespit edilen açıklar için sunulan çözüm önerileri de yine Scyther aracı ile tekrar analiz edilmiş ve önerilen yapının istenilen tüm güvenlik kriterlerini karşıladığı görülmüştür. Protokole yönelik olarak yapılan saldırılar ve sonuçları Tablo 2'de gösterilmiştir.

Burada önerilen protokol, diğer m-kupon protokolleri [14, 22] ile karşılaştırıldığında, güvenlik konusunda öne çıkmaktadır. Çünkü Alshehri vd. tarafından Dominikus ve Aigner'in çalışması [15] üzerinde yapılan analiz [27] ile yine Alshehri tarafından tez çalışması olarak Hsiang vd. tarafından yapılan çalışmalar [16, 17] üzerinde yapılan analizler [28] dışında diğer m-kupon protokollerinden güvenlik analizleri otomatik güvenlik protokolü 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.

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

KAYNAKLAR (REFERENCES)

1. Goggin G. Cell phone culture: Mobile technology in everyday life, Routledge, New York, A.B.D., 2012.
2. Krishna S., Boren S.A., Balas E.A., Healthcare via cell phones: a systematic review, Telemedicine and e-Health, 15 (3), 231-240, 2009.
3. 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 (1), 1-7, 2012.
4. Kwapisz J.R., Weiss G.M., Moore S.A., Activity recognition using cell phone accelerometers, ACM SigKDD Explorations Newsletter, 12 (2), 74-82, 2011.
5. Yıldırım K., Uçar G., Keskin T., Kavak A., Fall detection using smartphone-based application. International Journal of Applied Mathematics, Electronics and Computers, 4(4), 140-144, 2016.
6. Commission I.O. (n.d.). ISO/IEC 18092:2013: Information technology --Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1), 2013.
7. Bailey K., Plug in credit card reader module for wireless cellular phone verifications, Amerikan Patent Uygulaması No. 10/207,730.
8. 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, 59, 33-46, 2016.
9. 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. Springer, Cham. Vancouver, Kanada, 522-533, 9-14 Temmuz, 2017.
10. 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, Hırvatistan, 1-5, 15-17 Eylül, 2011.
11. 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. I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on. IEEE, Coimbatore, Hindistan, 828-833, 10 Şubat, 2017.
12. 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, 4(3), 258-262, 2016.
13. Hill S., Provost F., Volinsky F.C., Network-based marketing: Identifying likely adopters via consumer networks, Statistical Science, 21 (2), 256-276, 2006.
14. Hsueh S.C., Chen J.M. Sharing secure m-coupons for peer-generated targeting via eWOM communications, Electronic Commerce Research and Applications, 9, 283–293, 2010.
15. Dominikus S., Aigner M., mCoupons: An application for near field communication (NFC). 21st International Conference on Advanced Information Networking and Applications Workshops, 2007, AINAW '07, Niagara Falls, Kanada, 421-428, 21-23 Mayıs, 2007.
16. Hsiang H.-C., Shih W.-K., Secure mCoupons scheme using NFC. International Conference on Business and Information, 2008.
17. 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, 5 (11), 3901–3909, 2009.
18. 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, 7 (5), 131-138, 2013.
19. Hsiang H.C., A Secure and efficient authentication scheme for M-Coupon systems, 8th International Conference on Future Generation Communication and Networking (FGCN), Hainan, Çin, 17-20, 20-23 Aralık, 2014.
20. 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, 59, 204-217, 2016.
21. Yim J., Design of a smart coupon system, Multimedia and Ubiquitous Engineering, 11 (3), 187-198, 2016.
22. Jiang J., Zheng Y., Yuan X., Shi Z., Gui X., Wang C., Yao J., Towards secure and accurate targeted mobile coupon delivery, IEEE Access, 4, 8116-8126, 2016.
23. Bartoli A., Medvet E. (2016). An architecture for anonymous mobile coupons in a large network. Journal of Computer Networks and Communications, 2016.
24. 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, 52 (5), 710-725, 2015.
25. 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 Şubat 4, 2015. Erişim tarihi Aralık 25, 2018.
26. GSM Association, Mobile NFC Technical Guidelines-V2, 2007.
27. 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), Zürih, İsviçre, 1-6, 5 Şubat 2013.
28. Alshehri A.A., NFC mobile coupon protocols: developing, formal security modelling and analysis, and addressing relay attack. PhD Thesis. University of Surrey, 2015
29. Özcanhan M.H., Dalkılıç G., Utku S., Cryptographically supported NFC tags in medication for better inpatient safety, Journal of Medical Systems, 38 (61), 1-15, 2014.
30. Haselsteiner E., Breitfuß K., Security in near field communication (NFC), Workshop on RFID Security, Malaga, İspanya, 3–13, 11-13 Temmuz, 2006.
31. 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, 1-24, 2018.
32. Myerson R.B., Game Theory, Harvard University Press, 2013.
33. Cremers C.J., The scyther tool: Verification, falsification, and analysis of security protocols. International Conference on Computer Aided Verification, 414-418, Springer, Berlin, Heidelberg, Temmuz, 2008.
34. Lady E.L., Chinese Remainder Theorem, yayınlanmamış.
35. Montgomery P.L., A survey of modern integer factorization algorithms. CWI quarterly, 7 (4), 337-365, 1994.
36. Haraniya R., Sasmal C., Bopaliya B., Revar A., Comparative study of distributed online abatement, International Journal of Computer Applications, 165 (11), 25-28, 2017.
37. Reinhart L., Naatus M.K., Groupon, m-commerce and mobile apps: Perceptions of small business owners and consumers, Business & Entrepreneurship Journal, 6 (1), 27-38, 2017.
38. Chang C.C., Sun C.Y., A secure and efficient authentication scheme for E-coupon systems, Wireless Personal Communications, 77 (4), 2981-2996, 2014.
39. 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, 6 (3), 444-457, 2015.

40. Cremers C, Key exchange in IPsec revisited: Formal analysis of IKEv1 and IKEv2. In European Symposium on Research in Computer Security, 315-334, Springer, Berlin, Heidelberg, 2011.

41. Cremers C., Horvat M., Improving the ISO/IEC 11770 standard for key management techniques. In International Conference on Research in Security Standardization, 215-235, Springer, Cham, 2014.

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

43. Cas Cremers Selected protocol models for our analysis tools, https://people.cispa.io/cas.cremers/tools/protocols.html. Erişim tarihi Aralık 25, 2018.

44. Cas Cremers Publications, https:// people. cispa.io/ cas.cremers /publications/index.html. Erişim tarihi Aralık 25, 2018.

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

46. Görmüş S., Aydın H., Ulutaş G., Security for the internet of things: a survey of existing mechanisms, protocols and open research issues, Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (4), 1247-1272, 2018.

47. Okkalıoğlu B. D., Koç M., Polat H., Deriving private data in partitioned data-based privacy-preserving collaborative filtering systems. Journal of the Faculty of Engineering and Architecture of Gazi University 32 (1), 53-64, 2017.