TÜBİTAK

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2019) 27: 484 – 498
© TÜBİTAK
doi:10.3906/elk-1712-288

Formally analyzed m-coupon protocol with confirmation code (MCWCC)

Kerim YILDIRIM[1*], **Gökhan DALKILIÇ**[2], **Nevcihan DURU**[1]
[1]Department of Computer Engineering, Faculty of Engineering, Kocaeli University, Kocaeli, Turkey
[2]Department of Computer Engineering, Faculty of Engineering, Dokuz Eylül University, İzmir, Turkey

Received: 21.12.2017 • **Accepted/Published Online:** 29.11.2018 • **Final Version:** 22.01.2019

Abstract: There are many marketing methods used to attract customers' attention and customers search for special discounts and conduct research to get products cheaper. Using discount coupons is one of the widely used methods for obtaining discounts. With the development of technology, classical paper-based discount coupons become e-coupons and then turn into mobile coupons (m-coupons). It is inevitable that retailers will use m-coupon technology to attract customers while mobile devices are used in daily life. As a result, m-coupon technology is a promising technology. One of the significant problems with using m-coupons is security. Here it is necessary to ensure the safety of the seller's and retailer's data and to prevent unnecessary loss of income. In this study, a new m-coupon protocol is proposed and analyzed against well-known attacks: impersonation, man-in-the-middle, eavesdropping, replay, data modification, unauthorized coupon copying/generation, and multiple cash-in attacks. Then, to show that both the client and the retailer's data are at the highest level of security, the protocol is subjected to security analysis with a powerful protocol analysis tool, Scyther. Thus, the proposed protocol is proved to meet all safety criteria. To the best of our knowledge, this protocol is the first m-coupon protocol for which formal security analysis is conducted by the protocol's developers.

Key words: Authentication, data security, eavesdropping, formal security analysis tool, man-in-the-middle attack, m-coupon, near field communication, Scyther

1. Introduction

Mobile phones are now being used not only for communication but also to meet all daily needs. Day by day, new usage areas of mobile phones emerge. For example, companies and banks are trying to use mobile phones featuring near field communication (NFC) as credit cards [1]. Today, NFC is one of the major technologies of the Internet of Things (IoT) [2]. According to a Cisco white paper, 50 billion devices are expected to connect to the Internet by 2020 [3], which reflects the importance of IoT and NFC. Therefore, the leading mobile phone companies are adding the NFC feature to their phones; the iPhone has this feature with iPhone 6 and later versions [4]. This shows that mobile phones will play an important role in shopping. There are many other usage areas of mobile phones; some are still in their infancy stage while others are being used by almost everyone. For example, mobile phones are used as tickets for entertainment/transportation [5–7], or are used as mobile coupons to get discounts [8–13].

While customers are looking for cheap products and discounts, companies are trying to attract more customers and make them loyal. Companies' and customers' wishes intersect in coupons. There are three types of coupons: traditional paper-based coupons, electronic coupons (e-coupons), and mobile coupons (m-

[*]Correspondence: kerim_yildirim@yahoo.com

coupons). Among these types of coupons the most promising one is m-coupon because everyone has their own mobile phones all the time. The only thing you need to do is to tap the phone to get the discount. Thanks to m-coupons, companies can send any special offers to customers at any time and can abandon coupon printing and loyal card production/distribution.

In this work, we have developed a new M-coupon protocol with confirmation code (MCWCC), and to prove that MCWCC is secure we have analyzed the protocol with a formal security analysis tool, Scyther. We have also developed a web-based simulation of MCWCC by using JavaScript. The pseudocode of the simulation can be found at http://srg.cs.deu.edu.tr/publications/2018/mcwcc/. The paper is organized as follows: in Section 2, m-coupons are described and previous work is given. In Section 3, the proposed m-coupon protocol (MCWCC) is explained, and in Section 4 formal security analysis of MCWCC is executed.

2. M-coupons and previous works

M-coupons are stored on mobile phones to be exchanged when the customer wants to buy a product. M-coupons were announced a decade ago, but they are still in development. Companies and researchers are trying to increase the usage of m-coupons by developing new techniques and new secure m-coupon protocols [8–13].

M-coupons can be issued as a short message service (SMS) message [10], downloaded from an authorized m-coupon provider's page, transmitted via location-based services (LBS) [14], or published as a radio frequency identification (RFID) enabled poster. A general m-coupon protocol is given in Figure 1.

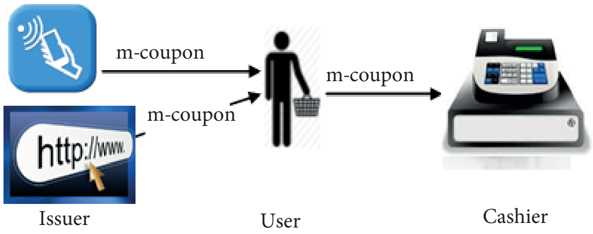


Figure 1. General m-coupon usage.

The advantages of using an m-coupon instead of the other coupons are as follows: it is easy to use, you always keep your mobile phone with you so it is not possible to forget it, it can replace loyalty cards easily, companies can make special discounts for special customers and can distribute the coupons at any time, your mobile phone can send you a notification while you are shopping where you can use your m-coupon, and dealers/companies can ensure that the coupons are used by the intended customers.

There are many m-coupon protocols. An NFC-based m-coupon protocol was proposed by Dominikus and Aigner in 2007 [11], and another NFC-based m-coupon protocol was proposed by Hsiang and Shih in 2009 [12]. In order to securely share m-coupons, the electronic word-of-mouth (eWOM) protocol was introduced in 2010 by Hsueh and Chen [10]; an NFC-based protocol, which can be used with low cost and constrained resources, was proposed by Park and Lee in 2013 [9]; and a lightweight cryptographic protocol to use in NFC posters with low computing capacity was also developed by Park and Lee in 2015 [13].

Hsiang for his protocol [8] used the protocol developed by Feldhofer et al. [15] and the protocol developed by Aigner et al. [16] as references and for comparison. The protocol developed by Feldhofer et al. [15] is a public key-based protocol and the customer takes the m-coupon from a passive NFC tag and then gives it to the cashier to get the discount. Aigner et al. [16] proposed a protocol with NFC technology and implemented it by using symmetric encryption algorithms. An almost new m-coupon system with its implementation was proposed by Yim [17].

All of these mentioned m-coupon protocols claim that they protect the rights of users and companies, the protocols are secure against attacks, and they provide sufficient security for users. However, there is no evidence to support these allegations or to prove that the protocols meet the desired security criteria.

While designing the protocol, to decrease the usage of asymmetric encryption algorithms and power consumption of mobile devices, we have used symmetric keys defined by the participants. With these symmetric keys, without using asymmetric encryption algorithms, we can check/confirm the message sender.

Additionally, and more importantly, to prove how secure the MCWCC is, we have analyzed our proposed protocol with a very powerful formal security analysis tool. As far as we know, MCWCC is the first m-coupon protocol that is analyzed by its developers with a formal security analysis tool.

3. M-coupon protocol with confirmation code (MCWCC)

Our proposed m-coupon protocol, MCWCC, which can be seen in Figure 2, is basically the same as the general m-coupon protocol model in Figure 3, where there are four participants: the manufacturer (F), coupon provider (P), user (U), and retailer (R). To use an m-coupon, first the user (customer) has to get an m-coupon (issuing phase), and then to get the discount, the user has to use the m-coupon (redemption phase). As the last step, the retailer who has given the discount to the customer sends a clearing request to the manufacturer to prevent multiple usage of the m-coupon (clearing phase). Notations used in the protocol are described in the Table.

Table. Notations of the scheme.

F	Manufacturer	ID_X	The identity of X; X = F, R, P, or U
R	Retailer	KU_X	Public key of X; X = F, R, P, or U
P	M-coupon provider	KR_X	Private key of X; X = F, R, P, or U
U	User/customer	K_{XY}	Symmetric key sent from user X to Y
MUC	Mobile device's unique code	K_{YX}	Symmetric key sent from user Y to X
M_C	Discount rate information	N_{XY}	Nonce, sent from user X to user Y
C_{ID}	M-coupon id	N_{YX}	Nonce, sent from user Y to user X
$H()$	Hash function	$E(..., KU_X)$	Encrypted by X's public key
$\|$	Concatenation	$E(..., KR_X)$	Encrypted by X's private key
O	Confirmation code	$E(..., K_{XY})$	Encrypted by symmetric key K_{XY}

3.1. The issuing phase

In the process of getting the m-coupon, the customer goes to the m-coupon provider (coupon provider's web site, NFC poster, etc.) and requests the coupon. As can be seen in Figure 2, the issuing phase consists of six steps and these steps are as follows:

Step 1. The user/customer (U) sends the identity information (ID_U) and a nonce (N_{UP}) to the coupon provider (P) to get the m-coupon as given in Eq. (1). The N_{UP} value will be used by U to check the identity of P.

$$ID_U \| N_{UP} \tag{1}$$

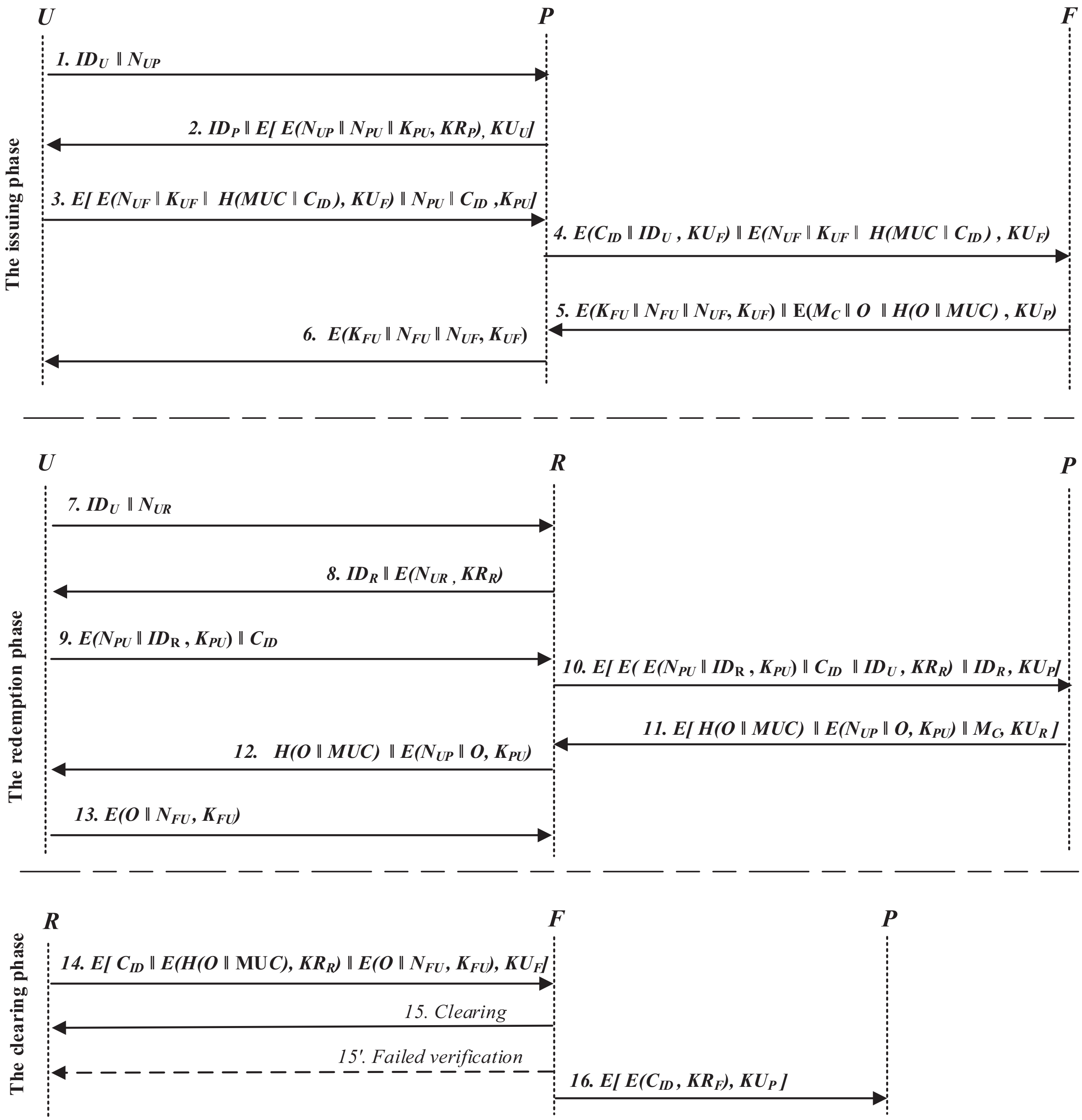

U
P
F
The issuing phase
1. $ID_U \| N_{UP}$
2. $ID_P \| E[\,E(N_{UP} \| N_{PU} \| K_{PU}, KR_P), KU_U]$
3. $E[\,E(N_{UF} \| K_{UF} \| H(MUC \| C_{ID}), KU_F) \| N_{PU} \| C_{ID}, K_{PU}]$
4. $E(C_{ID} \| ID_U, KU_F) \| E(N_{UF} \| K_{UF} \| H(MUC \| C_{ID}), KU_F)$
5. $E(K_{FU} \| N_{FU} \| N_{UF}, K_{UF}) \| E(M_C \| O \| H(O \| MUC), KU_P)$
6. $E(K_{FU} \| N_{FU} \| N_{UF}, K_{UF})$
U
R
P
The redemption phase
7. $ID_U \| N_{UR}$
8. $ID_R \| E(N_{UR}, KR_R)$
9. $E(N_{PU} \| ID_R, K_{PU}) \| C_{ID}$
10. $E[\,E(\,E(N_{PU} \| ID_R, K_{PU}) \| C_{ID} \| ID_U, KR_R) \| ID_R, KU_P]$
11. $E[\,H(O \| MUC) \| E(N_{UP} \| O, K_{PU}) \| M_C, KU_R]$
12. $H(O \| MUC) \| E(N_{UP} \| O, K_{PU})$
13. $E(O \| N_{FU}, K_{FU})$
R
F
P
The clearing phase
14. $E[\,C_{ID} \| E(H(O \| MUC), KR_R) \| E(O \| N_{FU}, K_{FU}), KU_F]$
15. Clearing
15'. Failed verification
16. $E[\,E(C_{ID}, KR_F), KU_P]$

Figure 2. M-coupon protocol with confirmation code (MCWCC).

Step 2. P calculates the N_{PU} and K_{PU} values to be used in the next steps. The N_{PU} value is a nonce that will be used to check the identity of U. K_{PU} is the symmetric encryption key to be used between U and P to encrypt the data to be transmitted in the next step. Thanks to these two values (N_{PU} and K_{PU}), P will be able to check the identity of U using a symmetric key algorithm. P adds the N_{UP} to the message to prove his identity and then encrypts it with his private key ($E(N_{UP}\|N_{PU}\|K_{PU}, KR_P)$). In order to check whether

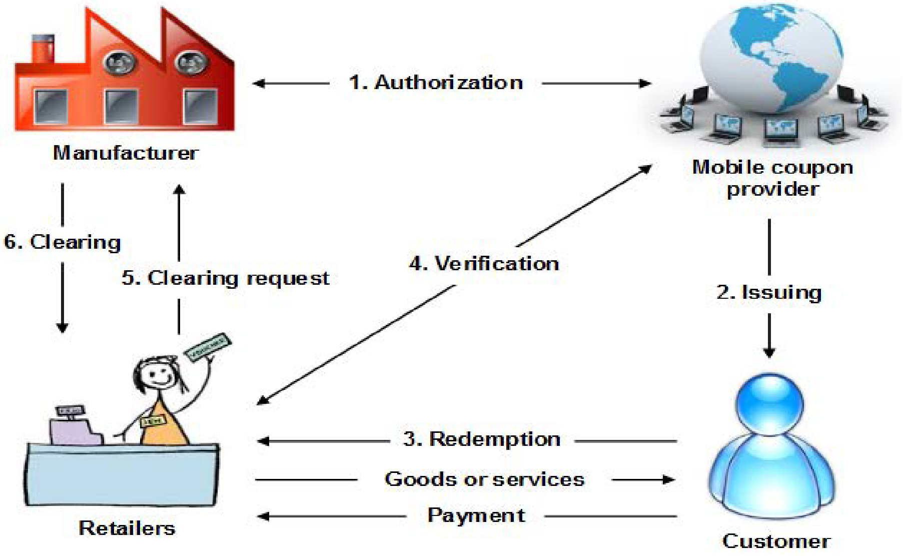


Figure 3. M-coupon protocol.

U is the correct user, it is encrypted with the public key of U. P also sends his identity ID_P to U with the message as in Eq. (2).

$$ID_P \| E(E(N_{UP} \| N_{PU} \| K_{PU}, KR_P), KU_U) \tag{2}$$

Step 3. After obtaining the ID_P value, U decrypts the message and obtains N_{UP}, N_{PU}, and K_{PU} values. The N_{UP} value was first sent by U to P so U checks the identity of P via the $N_{UP}{}'$ value. If the N_{UP} value is the same as the $N_{UP}{}'$ value, U confirms the identity of P.

U needs to calculate some values before getting the discount coupon. First, N_{UF}, K_{UF}, and ψ values are calculated. These values will be used with F in the next steps of the protocol. The N_{UF} value is a control value, the K_{UF} value is the symmetric key to be used between U and F, and the ψ value ($\psi = H(MUC \| C_{ID})$) will be used by F to check U's identity. Thanks to this value, the identity check of U can be proceeded without using the public key cryptosystem. The mobile device's unique code (MUC) value is a unique value that is created when U first joins F's loyal customer program and this value is only known to U and F. It defines U's mobile device. C_{ID} used here is the serial number of the m-coupon. By adding the C_{ID} to the hash summary, the ψ value will change in every session. Then U encrypts N_{UF}, K_{UF}, and ψ with F's public key to calculate the α value ($\alpha = E(N_{UF} \| K_{UF} \| \psi, KU_F)$).

U adds the N_{PU} value to the message, so that P will be able to check the identity of U. Also, she inserts the C_{ID} of the m-coupon and then the message is encrypted with the symmetric key (K_{PU}), which was sent by P in the second step ($E(\alpha \| N_{PU} \| C_{ID}, K_{PU})$).

P decrypts the message ($E(\alpha \| N_{PU} \| C_{ID}, K_{PU})$) with K_{PU} and obtains α, C_{ID}, and $N_{PU}{}'$, and then compares $N_{PU}{}'$ with the sent N_{PU}. If the two values are equal, U's identity is confirmed. After this step, α is just stored because it is encrypted with the public key of F as in Eq. (3).

$$E(E(N_{UF} \| K_{UF} \| H(MUC \| C_{ID}), KU_F \| N_{PU} \| C_{ID}, K_{PU}) \tag{3}$$

Step 4. So far, P has confirmed U's identity and obtained the serial number of the coupon that U

wanted. In this step, P encrypts the C_{ID} and ID_U with the public key of F, and then together with the data α sends the message to F as in Eq. (4).

$$E(C_{ID} \| ID_U, KU_F) \| E(N_{UF} \| K_{UF} \| H(MUC \| C_{ID}), KU_F) \tag{4}$$

P especially sends the ID_U of U to F. Thus, F can check U's identity, can confirm that P is not an intruder, and can be sure that there is a real customer requesting the m-coupon. F makes this check over the ψ value. F decrypts P's message. Using the obtained ID_U value, F finds the MUC value of U from his database. Then, by using MUC and C_{ID} values, he calculates $H(MUC \| C_{ID})$. If this value is the same as ψ, U's identity is confirmed. The N_{UF} value will be used by U to check the identity of F. The K_{UF} value is a symmetric key that will be used by F to send the data to U.

Step 5. After the verifications are completed, F calculates K_{FU} and N_{FU} values. N_{FU} will be used by F to check the identity of U. The K_{FU} value is the symmetric key that U will use to encrypt the confirmation code (O) in the course of the use of the m-coupon. F calculates the Ω value $(\Omega = E(K_{FU} \| N_{FU} \| N_{UF}, K_{UF}))$.

F sets a confirmation code (O) to check that the discount coupon is used by the intended customer. This code will be sent to U via P. Here, F does not only send the confirmation code (O) to U, but also sends the MUC and O values' hash summary. U recalculates the value of $H(O \| MUC)$ using the confirmation code (O) and the MUC value that it has. If the two hash values are the same, the confirmation code has been transmitted without error. Otherwise, the result shows that the confirmation code (O) is broken or manipulated on the way. F then adds the discount rate information (M_C) of the m-coupon and encrypts it with the public key of P, then sends it with Ω to P by using Eq. (5).

$$E(K_{FU} \| N_{FU} \| N_{UF}, K_{UF}) \| E(M_C \| O \| H(O \| MUC), KU_P) \tag{5}$$

Step 6. P decrypts the incoming message, separates the data to be retained in itself from the Ω value, and transmits the Ω value $(\Omega = E(K_{FU} \| N_{FU} \| N_{UF}, K_{UF}))$ to Uas in Eq. (6).

$$E(K_{FU} \| N_{FU} \| N_{UF}, K_{UF})) \tag{6}$$

To check the incoming message, U decrypts it with the symmetric key (K_{UF}), obtains the $N_{UF}{}'$ value, and compares it with his own N_{UF} value. If the values are the same, U understands that the sender is really F and keeps K_{FU} and N_{FU} for later use.

3.2. The redemption phase

To use the m-coupon, U must use his mobile phone and tap it to R's device. The redemption phase consists of 7 steps (Figure 2, steps 7 to 13).

Step 7. U sends his ID (ID_U) and a nonce (N_{UR}) to R's cashier ((Eq. (7)). The N_{UR} value will be used by U to check the identity of R as in Eq. (7).

$$ID_U \| N_{UR} \tag{7}$$

Step 8. The cashier encrypts (signs) the N_{UR} value with his private key $(E(N_{UR}, KR_R))$, adds his ID (ID_R) to the message, and sends it to U as in Eq. (8).

$$ID_R \| E(N_{UR}, KR_R) \tag{8}$$

By using R's public key, U obtains the $N_{UR}{}'$ value and compares it with her own N_{UR} value. Thus, U will be able to confirm the identity of the cashier.

Step 9. Until this stage, the cashier did not check U's identity. This check will be proceeded by P. To do this, U uses the N_{PU} and K_{PU} values sent to her by P in the issuing phase. To prove her identity, U adds ID_R to the N_{PU} value and encrypts it with K_{PU}. Then she adds C_{ID} of the m-coupon to calculate the λ value ($\lambda = E(N_{PU} \| ID_R, K_{PU}) \| C_{ID}$) and sends λ to R as in Eq. (9).

$$E(N_{PU} \| ID_R, K_{PU}) \| C_{ID} \tag{9}$$

Step 10. The cashier inserts the ID_U value into the incoming message and signs the message with his private key. Then he adds ID_R and encrypts the entire packet with the public key of P and sends the message to P as in Eq. (10).

$$E(E(E(N_{PU} \| ID_R, K_{PU}) \| C_{ID} \| ID_U, KR_R) \| ID_R, KU_P) \tag{10}$$

In this package, the ID_R value is sent twice. One of them is from U and the other one is from R. With these values, P can check if the cashier who is communicating with U and the cashier who is communicating with P are the same. In addition, the identity of U is checked by U's ID_U value. That is, to retrieve U's information from the records, P uses the ID_U and C_{ID} values sent by the cashier and finds K_{PU} and N_{PU} from the records. P decrypts the equation ($\lambda = E(N_{PU} \| ID_R, K_{PU}) \| C_{ID}$) by using K_{PU} and then compares the obtained $N_{PU}{}'$ value with the N_{PU} value he has sent. If the two values are the same, the identity of U is confirmed. He then checks the identity of the cashier using $ID_R{}'$. If the ID_R value sent by R is the same as the $ID_R{}'$ value sent by U, the identity of the cashier is also confirmed.

Step 11. Identity control of both U and R was done in previous steps. Now, P can send out the discount and control value to R. P encrypts N_{UP} and the control value (O) with the K_{PU} symmetric key ($E(N_{UP} \| O, K_{PU})$) to prove his identity to U. To obtain the ϕ value ($\phi = H(O \| MUC) \| E(N_{UP} \| O, K_{PU})$), P concatenates the hash summary $H(O \| MUC)$, which was sent by F, with the equation ($E(N_{UP} \| O, K_{PU})$), then adds the discount rate (M_C) value to the equation ($\phi = H(O \| MUC) \| E(N_{UP} \| O, K_{PU})$) and encrypts them ($E(\phi \| M_C, KU_R)$) with the public key of R as in Eq. (11).

$$E(H(O \| MUC) \| E(N_{UP} \| O, K_{PU}) \| M_C, KU_R) \tag{11}$$

Step 12. R gets P's message and decrypts it with his private key. He separates the discount rate (M_C) from the ϕ value and sends the ϕ value to U as in Eq. (12).

$$H(O \| MUC) \| E(N_{UP} \| O, K_{PU}) \tag{12}$$

U decrypts the encrypted data $E(N_{UP} \| O, K_{PU})$ with key K_{PU} and obtains $N_{UP}{}'$ and O' values. If the obtained $N_{UP}{}'$ is the same as the N_{UP} value that he already has, the identity of P has been confirmed. To check the obtained O' value, U takes the hash summary of MUC and O' values $H(O' \| MUC)$. If both digests are the same, O has not been changed along the way.

Step 13. U confirmed the identity of P and R, and that the control value (O) did not change along the way. Now she must report to F that she has received the discount. U encrypts the N_{FU} and O values with K_{FU} and sends the message to R as in Eq. (13). This message will be stored and then used by R in the clearing phase to prove that the discount has been given to U.

$$E(O\|N_{FU}, K_{FU}) \tag{13}$$

3.3. The clearing phase

R has given the discount to U and so lost some of the income. To get the lost income:

Step 14. R adds the hash summary $H(O\|MUC)$, sent by P, to the m-coupon serial number C_{ID} and signs them with his private key. He concatenates it to the data sent by U with equation $(E(O\|N_{FU}, K_{FU}))$ and sends it to F after encrypting with the public key of F as in Eq. (14).

$$E(C_{ID}\|E(H(O\|MUC), KR_R)\|E(O\|N_{FU}, K_{FU}), KU_F) \tag{14}$$

Step 15. F decrypts the incoming message and obtains the hash summary $H(O\|MUC)$. By using the obtained C_{ID} value, he finds U's data from the records. By using the K_{FU} value that he already has, he decrypts the data encrypted by U and obtains O' and $N_{FU}{}'$ values. If the obtained $N_{FU}{}'$ and N_{FU} values are the same, he compares the O' and O values. If these values are the same as well, he returns the discount to R as in Eq. (15). If the O' and O values are not the same, he compares the stored $H(O\|MUC)$ summary in his database with the hash summary $E(H(O\|MUC), KR_R)$, which R signed. If these two values are different, it is found that the corruption/error is in the communication between P and R, and if these two values are the same, it indicates that the corruption/error has occurred between R and U. This hash value has been added to the system to allow the source of the error to be detected.

$$CONFIRMED\,or\,FAILED \tag{15}$$

Step 16. Finally, to avoid the reuse of the m-coupon, F transmits the information to P that the coupon was used as in Eq. (16).

$$E(E(C_{ID}, KR_F), KU_P) \tag{16}$$

4. Formal security analysis of the protocol MCWCC

For a protocol to be claimed to be secure in a strong sense it is necessary to make a formal analysis of the protocol. The analysis of an m-coupon includes confidentiality, authentication, integrity, verifiability, unforgeability, and prevention of multiple usages of the coupon. The security of the m-coupon is a mandatory part of the protocol not only for the dealers but also for the customers, because dealers/companies may want to send special discount offers for special customers and want to ensure that only these intended customers can use these special offers. Also, they have to be sure that nobody can manipulate m-coupons as that can cause unnecessary losses. For the customers, they want to get the special discounts without any problem.

According to Mobile NFC Technical Guidelines [18] an m-coupon protocol should provide protection against attacks such as man-in-the-middle attack, eavesdropping, replay attack, data modification, unauthorized coupon copying/generation, and multiple cash-in [9]. Even without decrypting, just by intercepting or replaying the encrypted messages between the entities, some attacks can be applied. For example, in Alshehri and Briffa's work [19], which was a security analysis of Dominikus and Aigner's [11] protocol, communicating sequential processes [20] with model checker failure divergences refinement (FDR) [21] were used. They found some vulnerabilities and discovered some attacks to the protocol.

However, there is a significant point here that should not be overlooked: the formal security analysis of Dominikus' and Aigner's [11] protocol was conducted by some other researchers, not the protocol's designers. If, at the beginning, the security analysis had been conducted using formal security analysis tools, these vulnerabilities would have been avoided. Thus, to prove that our proposed MCWCC protocol is secure as we claimed, we have analyzed MCWCC by using the Scyther security protocol verification tool [22].

4.1. Security analysis of MCWCC

In this section, before it is analyzed with the powerful security protocol verification tool Scyther, we analyze the security of MCWCC against well-known attacks.

4.1.1. Resistance to impersonation attack

To prevent impersonation attacks, both public key encryption and nonce values are used. Public key encryption ensures that encrypted messages can be decrypted only by the private key owner and nonce values allow the sender and the receiver to verify each other's identity. For example, the N_{UF} value is sent by the customer to the manufacturer in step 3 of Figure 2; here, before sending, the nonce value N_{UF} is encrypted with F's public key ($E(N_{UF} \| K_{UF} \| H(MUC \| C_{ID}), KU_F)$), so that only F can decrypt it. Thus, U uses this value to verify the identity of F and looks for this N_{UF} value in the coming messages from F in step 6 of Figure 2. In addition, users know which nonce value will come, according to the recipient, and if the incoming nonce value is the same as the sent value, they understand that the sender is the expected user.

4.1.2. Resistance to man-in-the-middle attack

Even if the attacker is able to control all the traffic, he has neither the private key of any participant nor a symmetric key that he can use to decrypt the messages he obtains. The attacker cannot obtain the symmetric keys used in the protocol without having the private key, because symmetric keys are sent to the receiver encrypted using the public key. In addition, the messages are checked using nonce values as to whether they are coming from the expected user or not. If the values do not match, the communication will be terminated.

To prevent man-in-the-middle attacks, a security control value (O) is added to the protocol at the 13th step of Figure 2. With this step, the customer sends to the manufacturer the control value (O) to prove that she has received the discount. How the controls are made over the O value is described in detail in the 5th, 12th, and 13th steps of the protocol.

Another important security control method to prevent man-in-the-middle attack is sending ID_U and ID_R values to P. Both U and R send to P their identity to prove themselves. At the 9th step, U adds the cashier's ID_R value to the message for P as given in ($\lambda = E(N_{PU} \| ID_R, K_{PU}) \| C_{ID}$). Then, to prove his identity to P, R also adds his own ID_R value and ID_U value of the customer at the 10th step and sends them with the equation ($E(E(\lambda \| ID_U, KR_R) \| ID_R, KU_P)$) to P. After receiving the message, P decrypts it and checks the values N_{PU}, ID_U and ID_R. By using ID_U (this value is sent by R) and C_{ID} values, P finds K_{PU} and by using this key, decrypts $E(N_{PU} \| ID_R, K_{PU})$ and gets ID_R (this value is sent by U) and N_{PU} values. If $N_{PU}{}'$ value is equal to the sent value N_{PU} (this value is sent by P to U at the 2nd step of the issuing phase) the customer's ID is confirmed, otherwise it is determined that U is an attacker. Then, P checks ID_R value to find out who U is communicating with. If these two ID_R values are the same, then the R's identity is verified, otherwise it is determined that R is an attacker.

4.1.3. Resistance to eavesdropping attack

An attacker may listen to all the communication by eavesdropping; however, the attacker will not be able to get the contents of the message because confidential values sent to the receiver are encrypted and attacker has no keys to decrypt the encrypted data. The attacker can try to use the stored messages to perform a replay attack. However, this is also not possible as explained in the next subsection.

4.1.4. Resistance to replay attack

Separate nonce values (N_{PU}, N_{FU}, etc.) are created for each m-coupon and the data on m-coupon usage are recorded in the database by the manufacturer (F). Also, to prove his identity, the customer sends the hash summary of the coupon id (C_{ID}) and MUC values ($\psi = H(MUC \| C_{ID})$) to the manufacturer via the coupon provider at the 3rd step of the issuing phase. Thanks to the hash summary and nonce values, the manufacturer checks the identity of the customer. How this is performed is detailed in the issuing phase. Therefore, an adversary cannot replay eavesdropped messages from previous sessions to cheat any entity involved in the protocol. Even if the attacker tries to send the same messages again, since the information of the used m-coupon will already exist in the database, it will not be possible for the attacker to trick the system by replaying it.

4.1.5. Resistance to data modification attack

To secure communication and transferred data from eavesdropping or man-in-the-middle attacks, symmetric and asymmetric encryption and control values are used. The attacker must know either the private key of the participants or the key used for symmetric encryption in order to be able to change the content of the sent messages. Therefore, the attacker will not be able to obtain or change any secret data without knowing these keys. Even if the attacker tries to change it, the change will be noticed by the user through the use of the public key cryptography and through the nonce values.

4.1.6. Resistance to unauthorized coupon copying/generation attack

M-coupons are sent exclusively to customers, and the coupons that are sent can be tracked through the C_{ID} value. In addition, the customer also sends the hash summary of the requested m-coupon's C_{ID} value ($H(MUC \| C_{ID})$) to the manufacturer. C_{ID} values are stored in the database, and when the customer wants to use the m-coupon, this information is compared to the value stored in the database. Therefore, if the m-coupon is used or produced by a third party, it will easily be revealed.

4.1.7. Resistance to multiple cash-in attack

Reusage of an m-coupon is not possible, because the usage information is recorded in the database during the clearing phase and also the usage information is reported to the coupon provider. Even if the customer himself wants to use the m-coupon again, this situation will arise in the controls during the redemption phase, and the system will not give the discount because the coupon will be displayed as used in the database.

4.2. Security analysis of MCWCC with Scyther tool

Scyther is a very powerful tool, which is used for the formal analysis of security protocols. By making a finite representation of all possible protocol behaviors, Scyther can characterize the protocols. The tool, by providing brief representation of sets of traces, is based on a pattern refinement algorithm. This lets the tool aid the analysis of classes of attacks and possible protocol behaviors, and prove the correctness of the protocol [22].

Several protocols have been analyzed using the Scyther tool. For example, Taha et al. analyzed the IEEE 802.16 security sublayer [23], Basin et al. analyzed the ISO/IEC 9798 standard for entity authentication [24], and Cremer analyzed Internet key exchange protocols (IKEv1 and IKEv2) [25]. The most remarkable one here is the analysis of the IKEv1 and IKEv2 Internet key exchange protocols. IKEv2 protocol is widely used and details of the analysis made were shown by Cremer [25]. How the encodings and analysis are conducted is described in the Scyther Manual [26].

In Section 4.1, we claimed that MCWCC is secure against attacks and no attack can be found. To prove this claim, we have analyzed MCWCC by using Scyther v1.1.3 for MS Windows. This is not a trivial task and it is a process that requires very long and hard work to fulfill the necessary security criteria. In order to ensure that the protocol is secure, it is necessary to analyze each step of the protocol separately and then revise the protocol to remove the vulnerabilities detected by Scyther.

While analyzing a protocol with the Scyther tool, it is assumed that all the cryptography functions are perfect and an adversary cannot learn anything from an encrypted message without knowing the decryption key, and the protocol's steps are known. Thus, an intruder can interfere with the communication. The tool can check all attacks mentioned in Section 4.1.

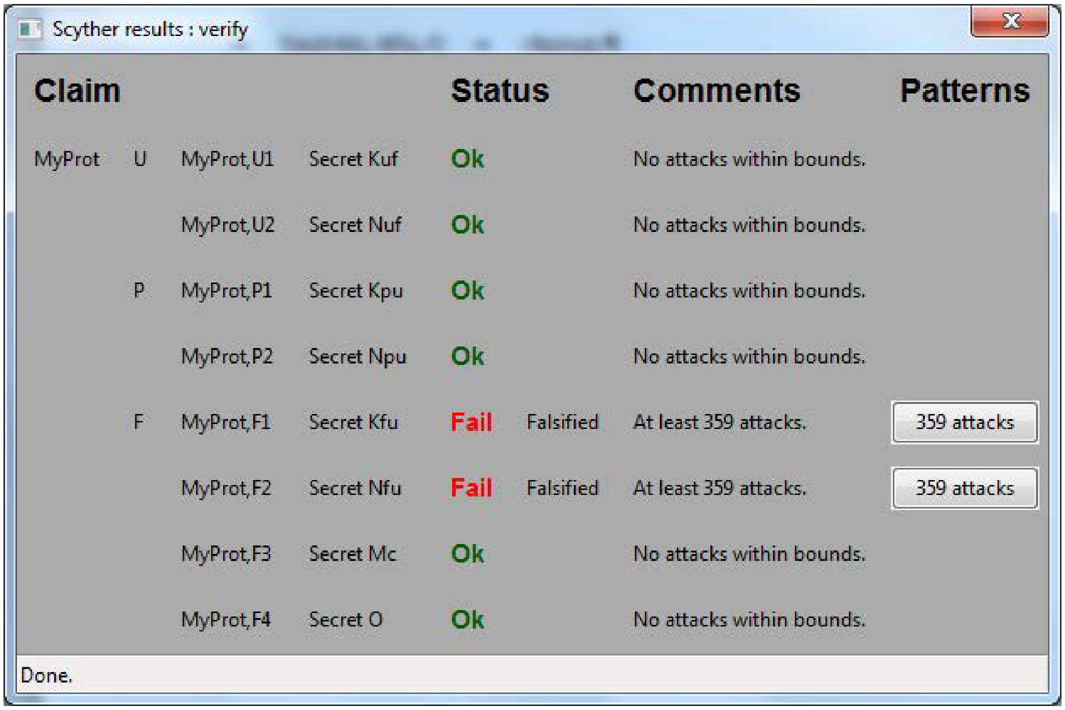
Before the analysis, according to the Scyther Manual [26], we identified the secret values that should be protected from an intruder. These values are nonces and symmetric keys. Then we encoded the issuing, redemption, and clearing phases according to the Scyther Manual [26]. We continued to work until each part was verified by the tool. If there exists a vulnerability in a phase, it may cause other vulnerabilities in other phases. Therefore, MCWCC's three phases are encoded together to find and analyze whether it is secure or not as a whole protocol.

In the security analysis of the early design of the protocol, two of the data (Kfu, Nfu) to be protected were attacked by the tool and the tool found 359 attacks. This is shown in Figure 4 and one of the attacks found by the tool is shown in Figure 5. In this attack, the intruder substitutes F, behaves like him, and interferes in the communication. Using his own Nuf (NonceIntruder1) and Kuf (SessionKeyIntruder1) values, the intruder obtains the symmetric key Kfu, which is generated by F. To prevent this attack, the MUC value is changed to a shared secret value [26], which means that the MUC value is known only by the customer (U) and the manufacturer (F). Therefore, while encoding, the MUC value is coded as a shared secret value "$k(U, F)$".

The MCWCC protocol is revised until no attack is found. As a result of very long and hard work, the MCWCC protocol is completed and the analysis conducted with the Scyther tool shows that the MCWCC protocol as a whole is secure and no attack has been found. The result of the verification is given in Figure 6. The Scyther tool source codes (MCWCC.spdl) can be found at http://srg.cs.deu.edu.tr/publications/2018/mcwcc/. These codes can be directly copied to the Scyther tool and can be verified by the tool.

5. Discussion

A study was conducted by Dickinger and Klijnen regarding the desire of customers to use m-coupons [27]. In that study, it was shown that the time and energy consumed for using m-coupons directly affects the use of the coupons. If the time spent to use the m-coupons increases, the desire to use the coupons decreases. It was also found that customers have a fear of spam and they are also cautious about the use of m-coupons because of the concern that their personal security will be in danger. Another research about m-coupon usage was conducted by Tercia and Teicher [28]. They examined customers' response to incentivized word of mouth and examined the effect of gender on preferences.

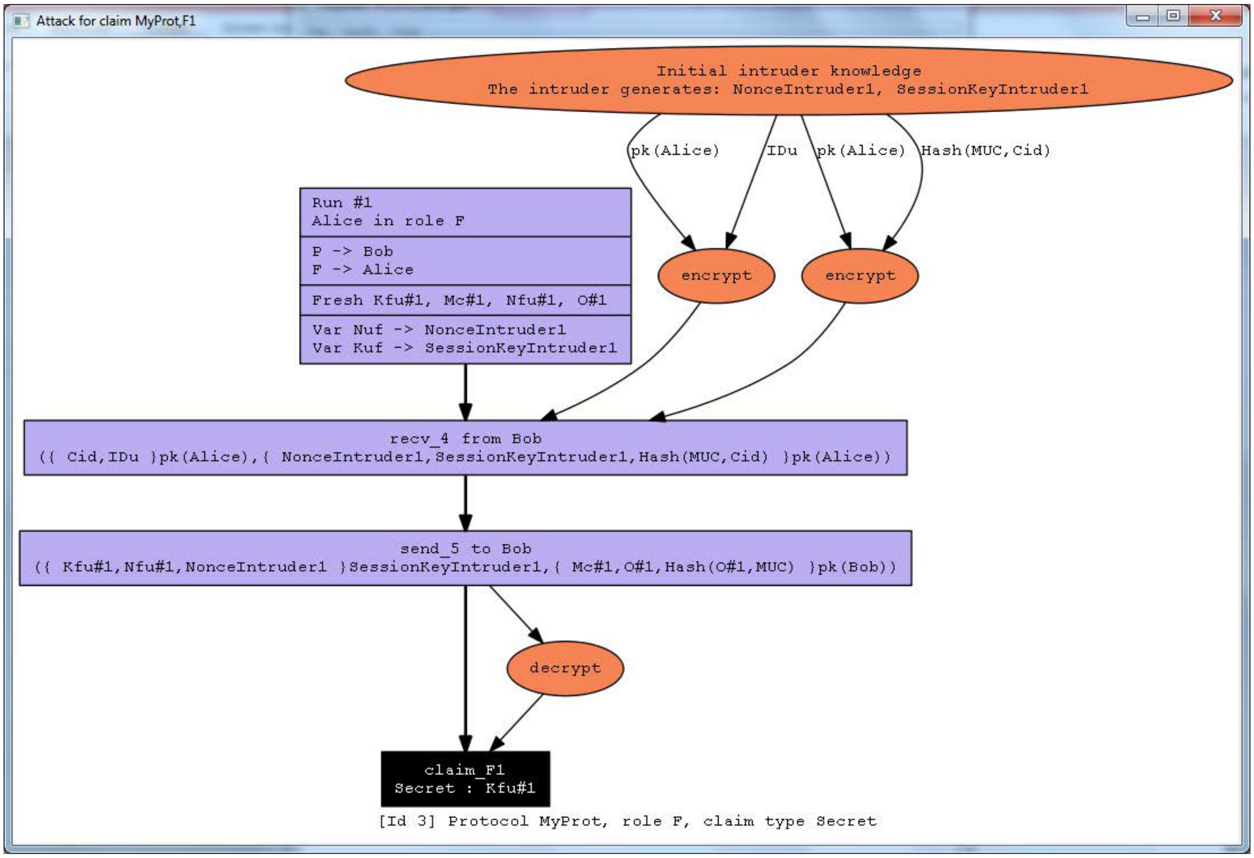


Scyther results : verify

Claim				Status		Comments	Patterns
MyProt	U	MyProt,U1	Secret Kuf	Ok		No attacks within bounds.	
		MyProt,U2	Secret Nuf	Ok		No attacks within bounds.	
	P	MyProt,P1	Secret Kpu	Ok		No attacks within bounds.	
		MyProt,P2	Secret Npu	Ok		No attacks within bounds.	
	F	MyProt,F1	Secret Kfu	Fail	Falsified	At least 359 attacks.	359 attacks
		MyProt,F2	Secret Nfu	Fail	Falsified	At least 359 attacks.	359 attacks
		MyProt,F3	Secret Mc	Ok		No attacks within bounds.	
		MyProt,F4	Secret O	Ok		No attacks within bounds.	

Done.

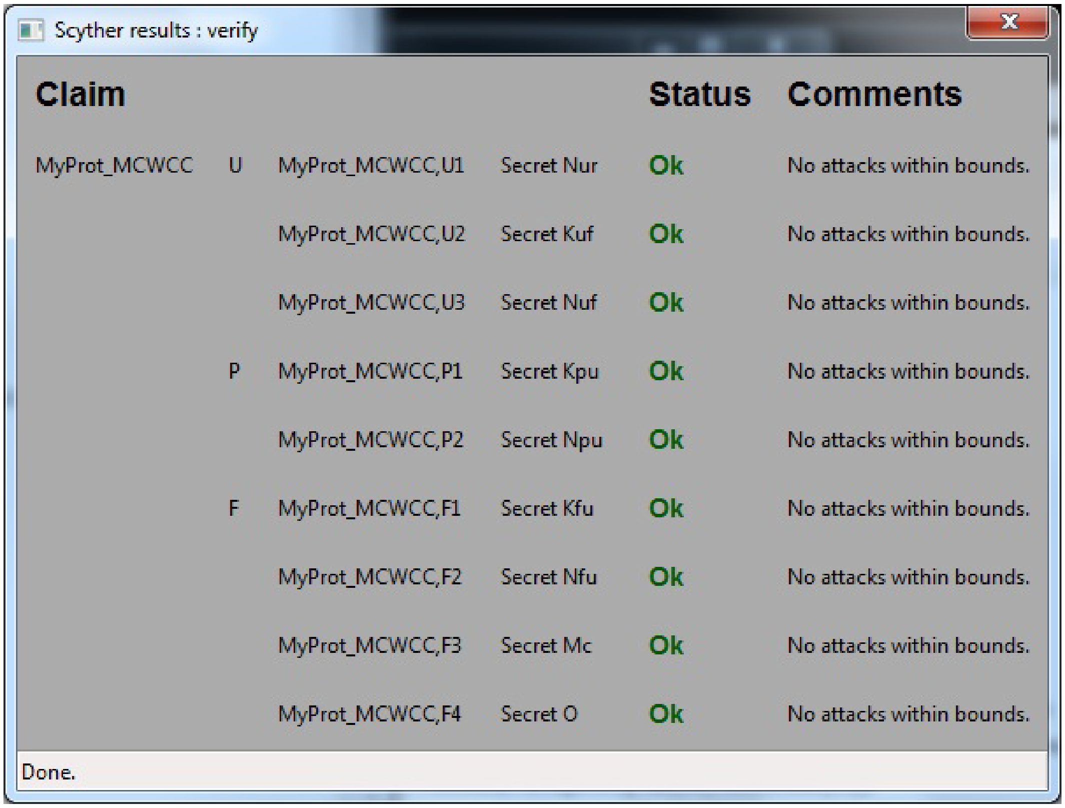
Figure 4. Early analysis results of the protocol.



Attack for claim MyProt,F1

Initial intruder knowledge
The intruder generates: NonceIntruder1, SessionKeyIntruder1
pk(Alice)
IDu
pk(Alice)
Hash(MUC,Cid)
Run #1
Alice in role F
P -> Bob
F -> Alice
Fresh Kfu#1, Mc#1, Nfu#1, O#1
Var Nuf -> NonceIntruder1
Var Kuf -> SessionKeyIntruder1
encrypt
encrypt
recv_4 from Bob
({ Cid,IDu }pk(Alice),{ NonceIntruder1,SessionKeyIntruder1,Hash(MUC,Cid) }pk(Alice))
send_5 to Bob
({ Kfu#1,Nfu#1,NonceIntruder1 }SessionKeyIntruder1,{ Mc#1,O#1,Hash(O#1,MUC) }pk(Bob))
decrypt
claim_F1
Secret : Kfu#1
[Id 3] Protocol MyProt, role F, claim type Secret

Figure 5. An attack against the protocol found by the Scyther tool.



Claim				Status	Comments
MyProt_MCWCC	U	MyProt_MCWCC,U1	Secret Nur	Ok	No attacks within bounds.
		MyProt_MCWCC,U2	Secret Kuf	Ok	No attacks within bounds.
		MyProt_MCWCC,U3	Secret Nuf	Ok	No attacks within bounds.
	P	MyProt_MCWCC,P1	Secret Kpu	Ok	No attacks within bounds.
		MyProt_MCWCC,P2	Secret Npu	Ok	No attacks within bounds.
	F	MyProt_MCWCC,F1	Secret Kfu	Ok	No attacks within bounds.
		MyProt_MCWCC,F2	Secret Nfu	Ok	No attacks within bounds.
		MyProt_MCWCC,F3	Secret Mc	Ok	No attacks within bounds.
		MyProt_MCWCC,F4	Secret O	Ok	No attacks within bounds.

Done.

Figure 6. Analysis results of MCWCC with Scyther tool.

However, nowadays contactless credit cards are increasingly used and transactions with contactless credit cards issued by banks have increased much more than transactions with regular credit cards. It can easily be said that the safety concerns of the users using contactless devices are reduced compared to a few years ago. At this point, it can be easily reached as a result that companies can take advantage of this opportunity and go more towards m-coupon applications.

As mentioned in the work done by Dickenger and Kleijnen [27], the most important point to note here is that companies should not overwhelm customers with m-coupons. Also, companies should make the right offer at the right time by analyzing the customer's gender, age, social environment, and shopping behavior and/or to attract customers can give a higher discount rate at times of lower shopping rates.

6. Conclusion

As mobile devices are a part of our lives, shopping culture has moved into new dimensions. In this context, the methods used by companies to attract customers are changing, and classic paper-based coupons used for discounting are also becoming mobile coupons. As we expect that the use of m-coupons will become widespread, in this study we have developed an m-coupon protocol, MCWCC, that would meet all the requirements of m-coupon security. Therefore, we analyzed it with a powerful formal security analysis tool, the Scyther tool. The output of this tool confirmed that the MCWCC protocol has a high level of security and reliability.

With the MCWCC protocol, customers can receive an extra discount at the cash register by using only their mobile devices without worrying about security. Also, we aim to make sure that, by using m-coupons, companies can safely give discounts to special customers without worrying about additional delivery cost. They will also save on the cost of card printing and distribution, because just a mobile device is enough to reach customers.

We have developed a web-based simulation of MCWCC by using JavaScript. The pseudocode of the simulation can be found at http://srg.cs.deu.edu.tr/publications/2018/mcwcc/. Our future work will be the implementation of the protocol with the Android operating system. We also plan to use elliptic curve cryptography in the protocol and measure its effect on performance.

References

[1] Tan GWH, Ooi KB, Chong SC, Hew TS. NFC mobile credit card: the next frontier of mobile payment? Telemat Informat 2014; 31: 292-307.

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

[3] 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.

[4] 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.

[5] Ghìron SL, Sposato S, Medaglia CM, Moroni A. NFC ticketing: A prototype and usability test of an NFC-based virtual ticketing application. In: 1st International Workshop on Near Field Communication; 24–26 February 2009; Hagenberg, Austria. pp. 45-50.

[6] Vives-Guasch A, Payeras-Capellà MM, Macia MP, Castellà-Roca J, Ferrer-Gomila JL. 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.

[7] 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. International Journal of Science and Technology 2012; 2: 817-822.

[8] Hsiang HC. A secure and efficient authentication scheme for m-coupon systems. In: 8th International Conference on Future Generation Communication and Networking; 20–23 December 2014; Hainan, China. pp. 17-20.

[9] Park SW, Lee IY. Efficient mcoupon authentication scheme for smart poster environment based on low-cost NFC. Int J Secur Appl 2013; 7: 131-138.

[10] Hsueh SC, Chen JM. Sharing secure m-coupons for peer-generated targeting via eWOM communications. Electron Commer R A 2010; 9: 283–293.

[11] Dominikus S, Aigner M. mCoupons: An application for near field communication (NFC). In: International Conference on Advanced Information Networking and Applications Workshops; 21–23 May 2007; Canada. pp. 421-428.

[12] Hsiang HC, Shih WK. Secure mcoupons scheme using NFC. Int J Innov Comput I 2009; 5: 3901-3909.

[13] Park SW, Lee IY. Light-weight authentication scheme for NFC mCoupon service in IoT environments. Lect Notes Electr En 2015; 354: 285-299.

[14] Chincholle D, Eriksson M, Burden A. Location-sensitive services: it's now ready for prime time on cellular phones! In: 4th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques; 25–28 June 2002; London, UK. pp. 331-334.

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

[16] Aigner M, Dominikus S, Feldhofer M. A system of secure virtual coupons using NFC technology. In: 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops; 19–23 March 2007; New York, NY, USA. pp. 362-366.

[17] Yim J. Design of a smart coupon system. Lect Notes Electr En 2016; 11: 187-198.

[18] GSM Association. Mobile NFC Technical Guidelines-V2, 2007.

[19] Alshehri A, Briffa JA, Schneider S, Wesemeyer S. Formal security analysis of NFC m-coupon protocols using Casper/FDR. In: 5th International Workshop on Near Field Communication; 5 February 2013; Zurich, Switzerland. pp. 1-6.

[20] Hoare CAR. Communicating Sequential Processes. New York, NY, USA: Prentice Hall, 1985.

[21] Ryan PYA, Schneider SA, Goldsmith M, Lowe G, Roscoe AW. Modelling and analysis of security protocols. New York, NY, USA: Addison-Wesley Professional, 2001.

[22] Cremers C. The Scyther tool: Verification, falsification, and analysis of security protocols. In: 20th International Conference, Computer Aided Verification; 7–14 July 2008; Princeton, NJ, USA. pp. 414-418.

[23] Taha AM, Abdel-Hamid AT, Tahar S. Formal verification of IEEE 802.16 security sublayer using Scyther tool. In: Network and Service Security, N2S'09 International Conference; 24–26 June 2009; Paris, France. pp. 1-5.

[24] Basin D, Cremers C, Meier S. Provably repairing the ISO/IEC 9798 standard for entity authentication1. IFIP Trans A 2013; 21: 817-846.

[25] Cremers C. Key exchange in IPsec revisited: formal analysis of IKEv1 and IKEv2. Lect Notes Comput Sc 2011; 6879: 315-334.

[26] Cremers C. Scyther User Manual. Oxford, UK: University of Oxford, 2014.

[27] Dickinger A, Kleijnen M. Coupons going wireless: determinants of consumer intentions to redeem mobile coupons. J Interact Mark 2008; 22: 23-39.

[28] Tercia CY, Teichert T. How consumers respond to incentivized word of mouth: an examination across gender. Austr Mar J 2017; 25: 46-56.