International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:2, 2016

Security Analysis of SIMSec Protocol

Kerem Ok, Cem Cevikbas, Vedat Coskun, Mohammed Alsadi, Busra Ozdenizci

***Abstract*—**Un-keyed SIM cards do not contain the required security infrastructure to provide end-to-end encryption with Service Providers. Hence, new, emerging, or smart services those require end-to-end encryption between SIM card and a Service Provider is impossible. SIMSec key exchange protocol creates symmetric keys between SIM card and Service Provider. After a successful protocol execution, SIM card and Service Provider creates the symmetric keys and can perform end-to-end data encryption when required. In this paper, our aim is to analyze the SIMSec protocol's security. According to the results, SIM card and Service Provider can generate keys securely using SIMSec protocol.

***Keywords*—**End-to-end Encryption, key exchange, SIM card, Smart card.

I. Introduction

LATEST SIM cards can provide secure end-to-end encryption between SIM card and Service Provider, since corresponding security keys are embedded to those –keyed– SIM cards at manufacturing phase by the Card Issuer (CI). However, most SIM cards those dispensed to the users today do not have embedded keys that can be used for end-to-end encryption between those –un-keyed– SIM cards and Service Provider.

End-to-end encryption between Service Provider and the Service Provider's application on SIM card is a must requirement for secure services. A Service Provider needs to be sure that no one can modify the communication conducted with the user. Data should be appropriately encrypted using a secure protocol using a proper key length. Considering the property of the SIM cards, using symmetric encryption protocols [1]-[5] is favorable.

In [6], we have provided SIMSec protocol, an end-to-end key exchange protocol, between an un-keyed SIM card and Service Provider in which both parties are not equipped with an encryption key at the beginning. The Service Provider can implement this protocol in its application and then can OTA load it to the SIM card with the permission of MNO. Then, Service Provider's application on the SIM card and the Service Provider's server can collaboratively create symmetric key pairs. When the keys are generated at both sides, Service Provider and SIM card can perform end-to-end encryption.

Cem Cevikbas is with Turkcell Technology (e-mail: cem.cevikbas@turkcell.com.tr).

Kerem Ok, Vedat Coskun, Mohammed Alsadi and Busra Ozdenizci are with NFCLab@Istanbul research laboratory, Information Technologies Department, Isik University (e-mail: kerem.ok@isikun.edu.tr, vedat.coskun@isikun.edu.tr, mehmet.alsadi@gmail.com, busra.ozdenizci@isikun.edu.tr).

This work is funded by TÜBİTAK (The Scientific and Technological Research Council of Turkey, www.tubitak.gov.tr/en) and Turkcell Technology (http://www.turkcellteknoloji.com.tr/) under TÜBİTAK project grant number 1505 – 5130053.

In this paper, we discuss SIMSec protocol's [6] security issues and perform security analysis using Casper/FDR tool [7]. The remainder of this paper is organized as follows. We give the related works in Section II. Section III includes the details of security analysis of SIMSec protocol and results. In Section IV, we conclude with implications of our study.

II. Related Works

SIM cards are classified as keyed and un-keyed. Keyed SIM card are manufactured according to the latest GlobalPlatform Card Specifications and are personalized during manufacturing phase to include required private keys. This enables security-requiring services such as digital signatures, mobile financial services to be provided after the SIM card is issued to a user. On the contrary, un-keyed SIM cards do not have any previously installed private keys to be used by the off-card entities for providing secure communication or any related services.

In order for a Service Provider to communicate with a SIM card securely, both parties should have encryption key so that they can encrypt data they send and provide end-to-end security. The issues related to end-to-end security issues are given in our previous work [8]. After, in [6] SIMSec protocol and its details is described creates an infrastructure for generating required keys at both sides using a key exchange protocol. The objective of the SIMSec protocol is to design a security infrastructure for enabling end-to-end encryption between the Service Provider and the SIM card. After this infrastructure is set up, Service Providers will be able to offer value added secure services to the users.

Research studies on smart cards are expanding in recent years especially with the introduction of emerging technologies such as NFC technology [9]-[11], Internet of Things [12], [13], and mobile payment systems [14], [15]. Additionally, the security of smart cards is also being studied in the literature [16], [17] and key exchange protocols are proposed as well.

In a study on the key exchange protocol for smart cards [18], authors proposed an end-to-end authenticated session key exchange protocol for SIM cards based on Secure Sockets Layer (SSL). The goal was to provide data integrity and confidentiality, and to reduce the cryptographic load for the SIM card by preventing exchange of plain text messages between the SIM and the OTA platform,

In another study [19], an authentication and session key distribution protocol is proposed for SIM cards those already include pre-installed keys. The proposed protocol provides end-to-end encryption between a keyed SIM card and Service Provider's Secure Access Gateway (a gateway to receive and send secure Short Message Service (SMS) messages). The authors also provide a formal security analysis of the proposed

protocol. Authors found out that the protocol ensures confidentiality between a SIM card and a Service Provider. The proposed authentication and session key distribution protocol deals only with the private key equipped SIM cards; hence it does not help solving our research problem for establishing a session key.

For analyzing the security of value added SIM card applications, some authors analyzed the security gap of traditional SMS based mobile commerce application model and designed a security model [20]. The model includes the authentication process, intercommunicative process between the SIM card and security access server, and the internal process of the security access server. This study assumes the integration of a private key in SIM cards prior to the execution of the protocol, hence does not help to solve our research problem.

In [21], a cryptographic protocol is proposed that provides secure entity authentication, data integrity, and data confidentiality. The protocol is based on Diffie-Hellman key exchange protocol and uses a combination of public key and secret key cryptography. The protocol provides mutual authentication and key establishment in a multi-application smart card environment. The authors study the protocol with the assumption that the Service Providers have a key pair; and the public key of each Service Provider's key pair is securely loaded to a security domain of the smart card. Then, they use the corresponding private key for the certification of RSA public encryption keys, which are further used for the establishment of a secure channel. This protocol assumes that private keys and digital certificates exist on the smart card before the key exchange, so does not help solving our research problem.

III. Security Analysis of SIMSec Protocol

SIMSec protocol is developed specifically for un-keyed SIM cards, which have low computing power, and allows only limited functions. 168-bit key is generated after protocol successfully runs which will be used in 3DES algorithm, and even 112 bit 3DES is assumed to be secure until 2030 by NIST [22]. Thus, using a 168-bit key in 3DES algorithm will enable a secure communication between Service Provider and SIM card. The generated key will be used to encrypt sensitive information and should provide desired security requirements. In this section, we give the threat model, security requirements of the SIMSec protocol and discuss possible threats.

A. Threat Model and Security Requirements

There are some possible threats that can challenge SIMSec protocol. While key is being exchanged between SIM card and Service Provider, an intruder may eavesdrop the communication and try to hack the generated key. In order to address all possible threats, the following security requirements are identified:

- Confidentiality of the key: An unauthorized third party, even MNO should not be able to discover the key.
- Data Integrity: During the key generation phase, any attempt to interfere and modify the data sent between the SIM card and Service Provider must be recognized by the receiver.
- Authentication of SIM card to Service Provider: Service Provider should be able to authenticate the SIM card during key exchange protocol.
- Authentication of Service Provider to SIM Card: SIM Card should be able to authenticate the Service Provider during the protocol.
- Man in the Middle (MITM) Attack Protection: An unauthorized third party –including MNO– should not be able to perform MITM attack in order to establish another key or to alter or modify the communication.
- Replay Attack Protection: When an unauthorized third party –including MNO– replays a packet, the receiver should terminate the protocol. When an unauthorized third party –including MNO– delays a packet more than the allowed lifetime, the receiver should terminate the protocol.

B. Discussion of the Threats

In SIMSec protocol, SIM card and Service Provider uses an SMS channel that is controlled by the MNO. Only V value is exchanged via an alternative communication channel. On the other hand, the exchange of ID_{SIM} value between MNO and Service Provider is performed using a secure communication channel. This secure communication channel generally exists between MNOs and Service Providers; otherwise they need to set it up.

There are three different attacker types that our protocol shall handle:

- An internal attacker from MNO: As an institution, MNO is assumed to be a trusted entity; however, MNO employees are not individually trusted and are considered as potential attackers. An insider may try to find out ID_{SIM} data, listen SMS channel, and even try to modify the communication.
- An attacker who knows public values: The SMS channel is assumed to be an unsecure channel. Therefore, we assume any attacker may attack the key exchange protocol with the knowledge of public g and p values.
- An attacker from another Service Provider: SIM card may have executed the key exchange protocol with another Service Provider previously, which makes the other Service Provider aware of ID_{SIM} data. Therefore, an attacker from that Service Provider may also attack the protocol with the knowledge of ID_{SIM} and the public values of g and p.

1. Confidentiality of the Key

In SIMSec protocol, an unauthorized third party including MNO should not be able to discover the key, thus should not be able to listen or alter the communication after the key is established. The key exchange protocol is developed based on Diffie-Hellman methodology. In this methodology, calculation of $(g^b)^a$ or $(g^a)^b$ values by an unauthorized third party without knowing numbers a and b is not possible. In order to generate the key, the attacker needs to calculate at least one of these numbers; so the confidentiality of the key between SIM card

and Service Provider is ensured.

2. Data Integrity

In SIMSec protocol, the receiver should recognize any modification to the data from an unauthorized third party. In steps 8 and 15 [6], Service Provider and SIM card checks the incoming hash value with the calculated one and recognize the modification in the data, if any. As a result, the protocol satisfies the integrity of the data between SIM card and Service Provider.

3. Authentication of SIM card to Service Provider

Service Provider authenticates the SIM card in the protocol by using V value in hash functions. Since V value is exchanged via a secondary authenticated channel and only the user of the SIM card has access to this channel, Service Provider authenticates the SIM card.

SIM card's id value is also used in hash functions. SIM card's id value is private and known only by the SIM card, the MNO, and the other Service Providers that SIM card run the protocol with. The MNO shares this data with the requesting Service Provider via a secure channel maintained between them prior to the protocol. When the SIM card sends a packet to Service Provider, the packet also includes the hash of SIM card's id as given in step 5 of the protocol; Service Provider checks the hash in step 8 and ensures that the V value is used by the claimed SIM card.

4. Authentication of Service Provider to SIM card

SIM card authenticates Service Provider by using V value in hash functions. Since this V value is exchanged via a secondary authenticated channel and only the SIM card user and the Service Provider knows the value, the SIM card authenticates the Service Provider.

5. Man in the Middle (MITM) Attack Protection

In the key exchange protocol, an unauthorized third party should not be able to perform a MITM attack. In SIMSec protocol, V value is created by the Service Provider for one time use only and exchanged with the SIM card user from a secondary communication channel as described in previous sections. The MNO does not control this channel and is not able to retrieve V value from this communication channel.

As it is seen in the protocol, when the SIM card sends a value to the Service Provider and when the Service Provider sends a value to the SIM card, V value is used in hash functions in steps 4 and 10. If an unauthorized party including MNO tries to perform a MITM, it needs to guess this value, which has around 2^{60} possibilities (10 characters long, 64 possibilities for each character). Since V value is used by the Service Provider and the SIM card for one time only, and if the Service Provider or the SIM card identifies an unequal hash in steps 8 or 15, the receiving party terminates the communication and a new V value needs to be generated. As a result, using V value protects the protocol from a possible MITM attack from an unauthorized party including the MNO. As the computing capabilities of attackers increases in time, the length of the V value can be increased accordingly.

6. Replay Attack Protection

In the protocol, the SIM card and the Service Provider accepts only one packet for exchanged V value. Thus, performing a replay attack by repeating a packet is not possible, since the receiver will reject it. Moreover, there is a small period that V value can be used, so when an unauthorized party performs a replay attack by delaying a packet, it is rejected after this period ends.

C. Security Analysis of the SIMSec Protocol

The security properties of the protocol are discussed in previous section. In this section, we analyze and verify the protocol's security against possible attack types.

In order to analyze and verify the protocol, we used Casper/FDR tool, which is defined in [7]. In Casper/FDR tool, user specifies the protocol into a script using more abstract notation similar to the notation that appears in academic literature and then this script is used to translate the protocol into Communicating Sequential Processes (CSP) code, which is suitable for checking using Failure Divergence Refinement (FDR) [7]. Afterwards, a FDR model checker analyzes CSP code.

In this subsection, we first give the protocol description *in Casper/FDR* and then we define the security requirements of SIMSec protocol in Casper/FDR tool. Finally, the result of the analysis with *Casper/FDR is presented.*

1. Description of the Protocol in Casper/FDR

SIMSec protocol is defined in SIMSec protocol and the corresponding source code is given in Fig 1.

2. Confidentiality of the Key

We model the confidentiality of the key security requirement in Casper/FDR tool as:

```
StrongSecret(A, key, [B])
StrongSecret(B, key, [A])
```

According to the specification, the SIM card claims that the key should be confidential with the Service Provider. In addition; the Service Provider claims that the key should be confidential with the SIM card. With the StrongSecret specification, the program checks whether the attacker is able to break the key at the protocol or not.

3. Authentication of SIM card to the Service Provider

We model the authentication of SIM card to Service Provider security requirement in Casper/FDR tool as:

```
Agreement(A, B, [key])
```

The code specifies that SIM card should be authenticated to the Service Provider, and both should agree on the value of key.

4. Authentication of Service Provider to the SIM card

We model the authentication of Service Provider to SIM card security requirement in Casper/FDR tool as:

```
Agreement(B, A, [key])
```

The code specifies that Service Provider should be authenticated to the SIM card, and both should agree on the value of the key.

```
#Description
0.    -> SIMcard : SP
[SIMcard != SP]
<cardMsg      :=      Exp(G,x);      h1Result:=
H1(SIMcard,v,cardMsg)>

1.  SIMcard -> SP : cardMsg % gx, h1Result
 [SIMcard != SP]
<dhKey := Exp(gx, y); spMsg := Exp(G,y);
   h1Result':= H1(SIMcard, v,gx);
   h2Result   :=   H2(SIMcard,v,gx,   Exp(G,y),
dhKey);
   key := H3(SIMcard,v, dhKey)>

2.  SP -> SIMcard : spMsg % gy, h2Result
[h1Result==h1Result']
<dhKey := Exp(gy, x);
   h2Result':=  H2(SIMcard,  v,  Exp(G,x),  gy,
dhKey);
   key := H3(SIMcard, v, dhKey)>
3.  SIMcard -> SP   : {key}{key}
[h2Result==h2Result']
```

Fig. 1 Description of the protocol in Casper/FDR

```
Starting FDR

Checking assertion SECRET_M::SECRET_SPEC [T=
SECRET_M::SYSTEM_S
   No attack found

Checking assertion SECRET_M::SEQ_SECRET_SPEC
[T=   SECRET_M::SYSTEM_S_SEQ
   No attack found

Checking assertion  AUTH1_M::
AuthenticateRESPONDERToINITIATORAgreement
_key [T= AUTH1_M::SYSTEM_1
   No attack found

   Checking assertion
      AUTH2_M::
AuthenticateINITIATORToRESPONDERAgreement
_key [T= AUTH2_M::SYSTEM_2
      No attack found

Done
```

Fig. 2 Output of the Casper/FDR script

5. Result of the Analysis

After analyzing the protocol with the developed script in Casper/FDR tool, no successful attack is detected and it is seen that the key between the SIM card and the Service Provider is generated securely. The output of the Casper/FDR is given in Fig. 2.

IV. Conclusion

In this study, we have analyzed the SIMSec protocol's [6] security. First, we have defined the threat model and security requirements, and then discussed these requirements. Finally, we have performed a formal security analysis using Casper/FDR tool. Our results show that SIMSec key generation protocol securely generates symmetric keys on SIM card and on Service Provider.

References

[1] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, *The Twofish encryption algorithm: a 128-bit block cipher*, New York, NY: John Wiley & Sons, Inc., 1999.
[2] J. Daemen, V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*, Secaucus, NJ: Springer, 2002
[3] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," In *Fast Software Encryption*, R. Anderson, Ed. U.K: Springer, 1994, pp. 191-204.
[4] W. Stallings, W, "The advanced encryption standard," *Cryptologia*, vol. *26(3)*, pp. 165-188, July 2002
[5] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM journal of research and development*, vol *38(3)*, pp. 243-250, May 1994
[6] K. Ok, V. Coskun, C. Cevikbas, B. Ozdenizci, "Design of a Key Exchange Protocol between SIM Card and Service Provider," in *Proc. of 23rd Telecommunications forum TELFOR 2015*, Belgrade, Serbia, 24-26 Nov ember 2015, pp. 281-284.
[7] Casper: A Compiler for the Analysis of Security Protocols. Available online: http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper/ (Accessed on December 2015).
[8] K. Ok, V. Coskun, R. C. Cevikbas, "Challenges and Risks for a Secure Communication between a Smartcard and a SP through Cellular Network," *International Journal of Advances in Computer Networks and Its Security*, vol 4(4), pp. 26-30, December 2014.
[9] V. Coskun, B. Ozdenizci, K. Ok, "The Survey on Near Field Communication," *Sensors* vol *15 (6)*, 13348-13405, June 2015.
[10] B. Ozdenizci, V. Coskun, K. Ok, "NFC Internal: An Indoor Navigation System," *Sensors* vol *15 (4)*, 7571-7595, March 2015.
[11] B. Ozdenizci, K. Ok, V. Coskun, "NFC Loyal for Enhancing Loyalty Services Through Near Field Communication," *Wireless personal communications,* vol *68(4)*, pp. 1923-1942, February 2013.
[12] L. Atzori, A. Iera, G. Morabito, "The internet of things: A survey," *Computer networks* vol *54(15)*, 2787-2805, April 2015.
[13] D. Palma, J. E. Agudo, H. Sánchez, M. M. Macías, "An Internet of Things Example: Classrooms Access Control over Near Field Communication," *Sensors*, vol *14*, pp. 6998-7012, April 2014.
[14] S. Karnouskos, "Mobile payment: a journey through existing procedures and standardization initiatives," *Communications Surveys & Tutorials*, vol *6(4)*, pp. 44-66, 2004.
[15] H. Rodrigues, R. José, A. Coelho, A. Melro, M. C. Ferreira, J. F. Cunha, M. P. Monteiro, C. Ribeiro, "MobiPag: Integrated Mobile Payment, Ticketing and Couponing Solution Based on NFC," *Sensors*, vol *14*, pp. 13389-13415, July 2014.
[16] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, 32(5), pp. 321-325, October 2010.
[17] C. T. Li, C. C. Lee, C. J. Liu, C. W. Lee, "A robust remote user authentication scheme against smart card security breach," In *Data and Applications Security and Privacy XXV*, Y. Li, Ed. Virginia: Springer, 2011, pp. 231-238.
[18] M. Badra, P. Urien, "Toward SSL integration in SIM SmartCards," in *Proc. of the Wireless Communications and Networking Conference*, Atlanta, 2004, pp. 889-893.
[19] H. Rongyu, X. Guolei, C. Chaowen, X. Hui, Q. Xi, Q. Zheng, "A PK-SIM card based end-to-end security framework for SMS," *Computer Standards & Interfaces*, vol. *31(4)*, pp. 629-641, June 2009
[20] Y. Li, M. Chen, J. Nie, J. "Mobile commerce security model construction based on sms," in *Proc. 7th International Conf. Wireless Communications, Networking and Mobile Computing (WiCOM)*, Wuhan, China, 2011, pp. 1-3.
[21] K. Markantonakis, K. Mayes, "A Secure Channel protocol for multi-application smart cards based on public key cryptography," in *Communications and Multimedia Security*, D. Chadwick, B. Preneel, Ed. U.K.: Springer, 2005, 175, pp. 79-95.
[22] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid, "Recommendation for key management-part 1: General (Revision 3)," NIST special publication, 2006.