Available online at www.elixirpublishers.com (Elixir International Journal)

Electronics Engineering

Elixir Elec. Engg. 65 (2013) 19844-19846

ISSN: 2229-712X

Cryptographically Secure Encryption Model for RFID Credit Card

Rohit Sharma[1] and P.K.Singh[2]

[1]Department of Electronics, College of Engineering, Teerthankar Mahaveer University, Moradabad.

[2]IIMT Group of Institution, Meerut.

ARTICLE INFO

Article history:
Received: 22 October 2013;
Received in revised form:
25 November 2013;
Accepted: 7 December 2013;

Keywords
RFID,
Privacy,
Proposed model,
Encryption process.

ABSTRACT

In RFID protocols, random numbers are mainly required to analyze tag answers in order to guarantee the privacy of the owner of the transponder. Our analysis looks at the feasibility of RFID tags for supporting Cryptographically Secure Pseudorandom Number Generators on their limited chip. Here we discuss about the cryptographic approach which we have used to improve the security of RFID credit card. Also we discuss about the random bit generator used in this cryptographic approach.

Introduction

Radio Frequency Identification (RFID) is an automatic identification technology in which a small transponder (tag), attached to an object (i.e. person, animal or product), receives and responds to radio-frequency queries from a transceiver (reader). Tags usually respond with a constant value which facilitates their association with their holders. An attacker may track a user's movements, putting location privacy at risk.

The inclusion of random numbers in tag answers may deter such attacks. In reality, however, mechanisms for random generation are often not as well designed as could be expected.

Requirements to make secure our system:

1. We should take the permission of the card holder before starting the transaction. If the card holder has the authority to give the permission for transaction with the RFID reader then the legitimate can not exceeds the use of their RFID credit card reader.
2. We should perform a sophisticated encryption, which provides heavily confusion and diffusion to the adversary.

This model performing all these requirements that uses a very sophisticated encryption, that provide the confidentiality to our system and it also provide the large amount of confusion and diffusion to the adversary.

We know that card and card reader share the two track information for transaction.

An RFID credit card used a data format, in which card should contain their CVC value hidden.

Means card should contain total of three in formations.

1. Track1
2. Track2
3. CVC value

Than we should apply some cryptographic approach on these three track information. In this model we used two sensors, one random value generator, and RFID card and reader. Second sensor can only interact with the first sensor, random bits generator, and RFID credit card reader. First sensor operates opens in air to detect the RFID card. And RFID reader remains deactivated until it receive the signal from second sensor. RFID reader operates on the basis of command by second sensor.

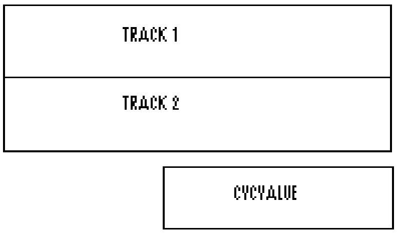


Fig 1: RFID credit card data format

Proposed model:

In this paper we have proposed architecture for encryption model. Proposed architecture containing two sensors with a random bit generator. RFID reader deactivated until it receives any command from second sensor. In this model, the first RFID sensor will used to search the RFID tag. When any RFID card comes in the range of this sensor than card sends their CVC value to it. First RFID sensor than forward this CVC value to second sensor. At the same time, when second sensor receiving the CVC value, it command for random bits to the random bits generator. Card will forward these CVC and random bits to the RFID reader.

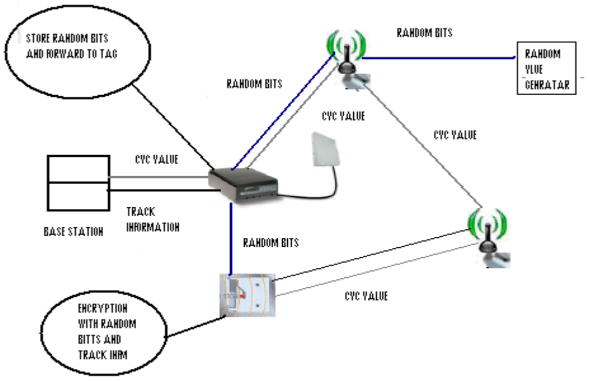


Fig 2: Proposed encryption model to make system more secure

Tele:
E-mail addresses: rohit_techelectro@yahoo.com

RFID reader firstly stores the random bits in the memory and forwards it to the card. On other hand, at the same time reader request to base station for track information of card by sending the CVC value. Point is noted that the track information sending by the base station is same as store in card.

After all these process, card has the two track value, random bit and CVC value.

Same three values have present at the RFID reader. Now we perform the encryption process on these values in the card with the help of small microprocessor chip. Same process will perform at the RFID reader. After the completion of encryption process, card will send the encrypted data to the reader. As we know that same process has done at the RFID reader. In this process two causes are occurring, first case when both data will match then the transaction will occur. If data will not match the transaction will be terminate.

In the complete process we will not consider the CVC value as the part of encryption process. Because the CVC value have openly announced. Then CVC value can be helpful for the adversary to break encrypted code. But if we use CVC value at last for encryption than it's not beneficial for adversary.

Encryption process: Block diagram for the encryption process used in the encryption model is shown in figure 3. In the complete process we use three hash functions. First hash is use to digest the content of track 1 data. Second hash function is used to digest the content of track 2 data. Third hash function will digest the combination of hash function 1 outputs and hash function 2 outputs.

Operation performed by all these three hash functions will be different with respect to each other. The output of the third hash function will be encrypted with the help of the CVC value of card.

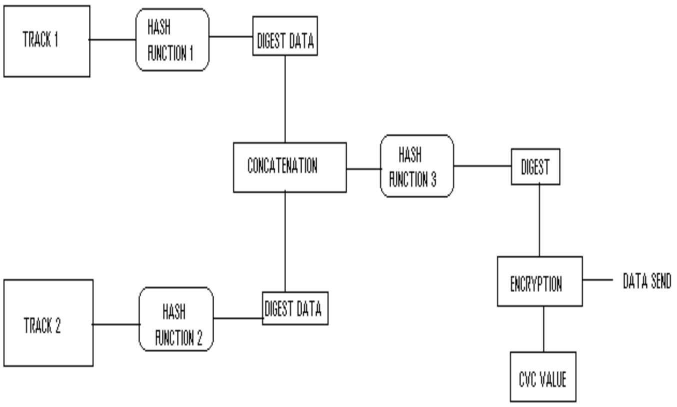


Fig 3: Working of encryption process in encryption model

Data digest: In the block diagram, the track 1 and track 2 data is digest by using the hash algorithm. Now we describe the operation of hash algorithm and how it digests the data with the help of random bits generated by the generator. Before starting the operation we need to share some important point:

1. The length of the track data should be divided into equal size of block.
2. The size of random bits generated by the generator must be equal to size of track data block.
3. Here the approach used for hash function is different, we use here the block of track data as a secret key and random bits are used as a message.

These are the three main points which lead our encryption model. Now we tour about the working of our encryption algorithm.

Block diagram of a track 1 data is shown in figure. In this architecture, we take the random bit as a message sequence and track data as a secret key.

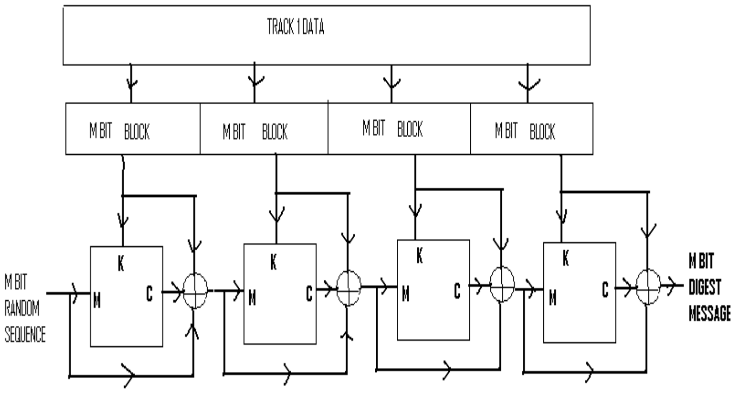
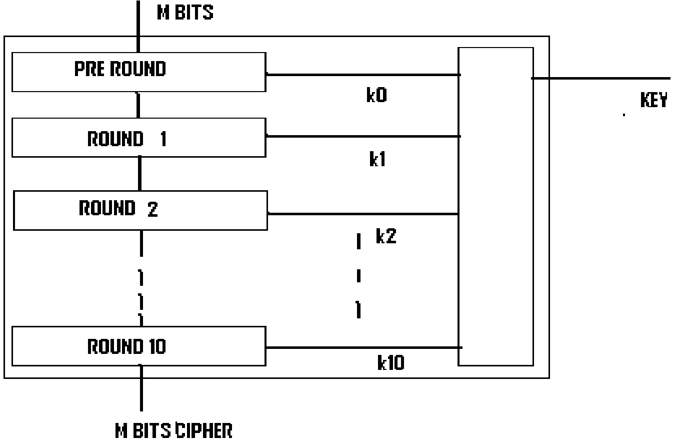


Fig 4: Data digest with the help of random bits

In this algorithm, we divided the track data into the equal number of blocks. The length of the random sequence is equal to the length of data block. We can see that each block apply to the digest algorithm with the random sequence and the output of the first block is apply as a message to the input of second block and so on. The same process is applied for all blocks than the output we get is the digest form of track data equal to the size of block.

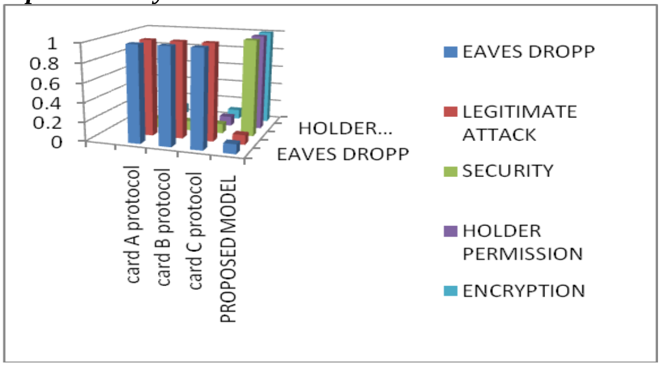
Here we can increase the confusion for adversary. We can see that each step generating the chipper with the help of message and key. And each step generates a chipper by performing number of rounds. If we increase the number of rounds then confusion will increase for adversary.

In our approach we use only 11 rounds. Each round performing a different operation.



This is the 11 round operations to generate the chipper. 11 keys will be used to generate the cipher. Each round performing the different operation the cipher text is the combination of multiple numbers of operations. Similarly each operation will be performing on each block of data.

Graphical Analysis



Conclusion: In this paper we have discuss an encryption model to improve the security of RFID credit card. This model has the ability to provide the diffusion and confusion to the adversary. This model can also help us to build RFID in global environment.

Comparative Analysis

Only the protocols model have deployed by the researcher for RFID credit card security. I have compared these protocols with our proposed model.

Analysis by table

Factors	**Eaves dropping**	**legitimate attack**	**security**	**Holder permission**	**Encryption**
card A protocol	YES	YES	LESS	NO	NO
card B protocol	YES	YES	LESS	NO	NO
card C protocol	YES	YES	MODERATE	NO	NO
proposed model	NO	NO	HIGHER	YES	YES

Reference:

1. J. Daemen and V. Rijmen, *AES Proposal: Rijndael*, “AES Algorithm” Submission, September 3, 1999.
2. J. Nechvatal, et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.
3. Card Technology: Paypass subway trial starts in New York (2006) http://tinyurl.com/uya3k.
4. Carey, D.: NFC turns phone into a wallet. EE Times (2006) http://tinyurl.com/yyxk28 Last Viewed October 8, 2006.
5. EMVCo: EMV Integrated Circuit Card Specifications for Payment Systems. (2004) http://tinyurl.com/oo663 Last Viewed October 11, 2006.
6. Hancke, A practical relay attack on ISO 14443 proximity cards. Technical report, University of Cambridge Computer Laboratory (2005) http://www.cl.cam.ac.uk/˜gh275/relay.pdfLast Viewed October 12, 2006.
7. Harper, RFID wiggles its way into credit cards?(2005) http://lists.jammed.com/politech/2005/05/0038.html.
8. ISO: ISO/EIC 14443, proximity cards (PICCs). Technical report, ISO (2006) http://wg8.de/sd1.html.
9. H. Chan, A. Perrig, and D. Song “Random Key Pre-distribution Schemes for Sensor Networks”, Proc. IEEE Symposium on Security and Privacy, pp. 197-213, 2003.
10. W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Pairwise “Key Pre-distribution Scheme for Wireless Sensor Networks”, Proc. ACM Conference on Computer and Communication Security, CCS'03, pp. 42-51, 2003.
11. L. Eschenauer, and V. D. Gligor “A Key-Management Scheme for Distributed Sensor Networks”, Proc. ACM Conference on Computer and Communication Security, CCS'02.
12. S. Ganeriwal, S. Ravi, and A. Raghunathan “Trusted Platform Based Key Establishment and Management for Sensor Networks”, Under Review.