Research Article

Literati Journals
Empowering Researchers

Security for EMV Card Data in Payment Systems

Satish Kabade,[1]* Meenakshi Sundaram[1]

Abstract: The remote senses generate very large amount of real time data from the Satellite or from the Aircraft with the help of the sensors. Now a day there is a great demand added to the real time big data for remote sensing applications, these data has to be processed and extract the useful information can lead to computational challenges. From these above mentioned factor need to design an architecture that can supports both offline as well as the real time data. In this paper we will discuss the proposed architecture for the remote sensing application. The three main units comprises the proposed architecture the three units are First, Remote sensing data acquisition unit (RSDU) takes the data from the satellite and sends to the Base Station, where processing starts in this unit. Second, Data processing unit (DPU) is the main role in the architecture, the real time data will process efficiently by filtering, load balancing and parallel processing and Third, Data Analysis and Decision unit (DADU) this unit is responsible for the storing the results and generates the decision based on the results of the data processing unit. The proposed architecture can store raw data for the analysis of the offline data when required.

Asian Journal of Engineering and Technology Innovation
Volume 4, Issue 7
Published on: 7/05/2016

Cite this article as: Satish Kabade and Meenakshi. Sundaram Security for EMV card data in Payment Systems. Asian Journal of Enginnering Technology and Innovation, Vol 4(7): 116-119, 2016.

INTRODUCTION

The credit card system has supported innovation for over a period of 50 years. That is the reason they succeeded in any case. Amid the 60s and 70s, they contended with cheque cards that a client could use to ensure a cheque to any trader up to a specific sum. MasterCard won this opposition, and the primary reason was that they had the adaptability to adjust to mail request and sales order form telephone. The card companies found that they would build not only a settlement system but also a global system of authentication where the client name was the card number, and password the expiry date (joined from the early 1990s by CVVs).

There is currently a column fermenting over the new EMV chip card framework grew mutually by Euro pay, MasterCard and Visa through EMVCo from 1995 onwards.In the course of recent years EMV has been sent in the majority of Europe and is beginning to show up in different nations, for example, Canada and India.. This present year US will end up being the last G20 nation to move to EMV innovation which influences a chip installment card rather than attractive strip to verify an exchange. Advantage of EMV lies in the dynamic nature information, as the chip makes a one of a kind code for every exchange.

[1]Reva Institute of Technology and Management, Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Near Border Security Bustop, Bengaluru, Karnataka-560064, India.
E-mail: ashwin@revainstitution.org
*Corresponding author

The development of phishing assaults on electronic saving money since 2005 prompted the improvement of the Chip Authentication Program (CAP). The convention empowers a bank to utilize its issued base of EMV cards to create to bolster twofold element verification: it furnishes every costumer with a little minimal effort pursuer, and when the client sign on to the bank site she is requested with a validation code which she can produce by embedding her card in the CAP reader and punching her PIN.

Once we must holds with the crypto conventions utilized as a part of EMV, we would ask what advancements can be conceivable with EMV that does not require any banks to change their Systems by any stretch of the imagination.

Regardless of the possibility that a cryptographic convention outline is extremely stable, the coding and usage might be imperfect, there might be constantly a few escape clauses; principals might be not be straightforward; or different principals might make question about one's honesty or framework segments. Such issues every now and again happen with budgetary exchange conventions, where genuine cash is in question.

Magnetic Stripe card is less secure as hackers can clone the card easily. Issuer has to pay for the fraud of any case. Why not encrypt the data of readcard with PIN entered so that data can be authenticated and more secure. This is one way of securing Magnetic Strip card. However EMV won't be sufficient to lessen MasterCard fakes. Security ought to be given in layered methodology. At the point when utilized as a part of conjunction with right encryption approach and utilizing

information and terminal encryption considerable security would take out card holder extortion from trader environment. End to End encryption is depended upon to rise by 151% percent before the end of 2016, and the use of tokenization will increase by 130 percent before the end of 2016.

LITERATURE SURVEY

EMV(which we know stands for EuroPay, MasterCard and Visa) is a smart card system deployed all over the world, is extensively set up in Europe and ready to be introduced in the US as well.Inspite of this wide setup , there are various liabilities which make EMV defenseless against the preplay attack. To be particular weak calculations used to generate random numbers, deficient calculations and numerous protocol failure leave the system prone to fraud or hackers.

Security protocols which are used to authenticate numerous transactions, generally end up in lawful suits. Designers very often fail to foresee this. In this paper we show how the EMV protocol which is a robust card payment system, does not produce satisfactory proofs to fix the disputes. Five principles are proposed to design systems to produce exceptionally solid evidence. We apply these to different systems, for example, Bit coin, electronic Banking and POS. At last we propose specific changes to EMV framework which can resolve disputes decently and with much more proficiency.

EMV is also known as “chip and pin card” is leading payment card all over the world. It is widely used in Europe and much of Asia. This is going to be introduced in U.S. Chip in payment card acts as an authentication protocol. Chip along with the pin generate a nonce, an unpredictable random number which ensures each transaction is unique. Some authors have discovered two serious problems.

1. The first flaw being the generation of the nonce .The implementers have just merely used counters, home grown algorithms and timestamps, which makes the EMV systems vulnerable to hackers and “preplay” agents. This flaw facilitates card clones using the logs available in card issuing bank. The purpose of EMV invention itself is defeated here.Flaws were found in the widely used ATM also. There were reports of frauds where in victims were refused their refund as the notion was it was impossible to clone the card, but the fraud can be easily explained now.
2. The second problem is protocol failure. The nonce generator can simply be replaced by attacker making significantly vulnerable.

PROBLEM STATEMENT

The card data generated from reading any payment card is critical to user as well as to the card issuer. This data already encoded by EMV data using TLV tags. This tags containing the encoded data can be continuously changed so that its becomes very hard for hackers to attack .The read card data itself can be encrypted using robust algorithms like ASA , RSA And ADES algorithms so that it will be impossible for hackers to attack the system.

NEED FOR EMV CARD AND SECURE MAGSTRIPE CARDS

With progression of innovation, Credit card fraud turned into a noteworthy concern. Attractive strip cards turned out to be profoundly defenseless in the most recent couple of years. Small gadgets could be utilized to rapidly swipe a credit card, duplicate all the data on it and utilize that to make a fake duplicate.

The devices started emerging everywhere –in ATMs, inns, and in metro stations. Because of this, banks were enduring substantial losses. The fraudulent charges were secured by the card issuer, since laws shielded purchasers from obligation. Because of this, more Visa organizations around the globe started to change their cards to the EMV standard. Rather than putting away individual data on a magnetic strip, EMV-good cards hold all basic information on a coordinated chip. This information is encoded and continually changing, making it fundamentally harder to fake. The advantages of EMV standards spread like wildfire. As per the statistics of December 2013 and data from EMV Connection, 99.9% of point-of-sale terminals in Europe use EMV. Notwithstanding it, more than 70% of terminals in Asia, Africa, the Middle East, Canada, and Latin America additionally adhere to the EMV standard. Another way of avoiding fraud is use of secure Magstripe cards. The data fetched from the SWIPE are encrypted so the hackers cannot counterfeit. When PIN information made mandatory, PIN used as a key in encryption the data become very hard to hack.

IMPLEMENTATION AND DESIGN

The papers explains the implementation by using host device and payment hardware. It explains the communication model, design and architecture, data flow between entities and finally the results.

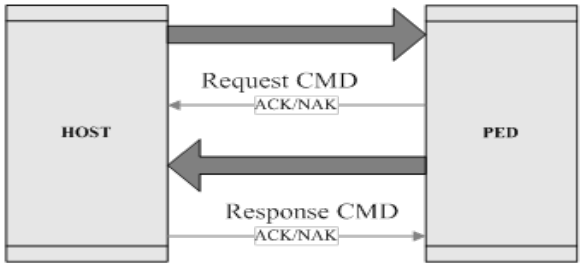

Figure 1: Communication between entities

The host is any android device. The PED is PIN entry device which is the payment hardware. The communication

between the host and PED is through Bluetooth. It follows Bluetooth SPP profile i.e. command based messaging for communication. That is through requesting command and receiving the response.

Using ECI Communication Interface mode: for each communication packet, after it is received correctly, receiving end requires an immediate response ACK characters, or response NAK. If the sender doesn`t receive ACK or NAK within 2000ms after sending a packet, you need to try again four times

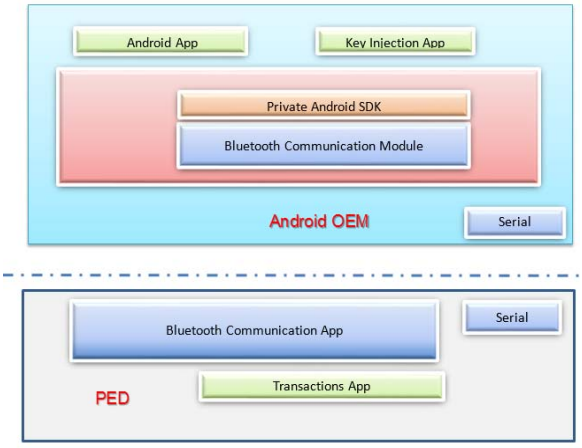

Figure 2: Design and Architecture

Layered Architecture

The OTS system architecture is a layered approach design between Android module and the PED. The Android module has to use the Bluetooth component API to communication between the PED hardware. The payment framework is the module which talks to PED hardware using protocol model shown in above figure. This is command based message communication through Bluetooth SPP profile.

Bluetooth communication module of android device and Bluetooth communication app of PED hardware always talk through Bluetooth SPP commands. Key injection app and Android application can be a common application. Key injection app is used to download RSA key into the PED.

Using ECI Communication Interface mode: for each communication packet, after it is received correctly, receiving end requires an immediate response ACK characters, or response NAK. If the sender doesn`t receive ACK or NAK within 2000ms after sending a packet, you need to try again four times.

Encryption Solution

Readcard method reads the card data from the PED device furthermore, subsequent to handling gives back the information in the TLV (Tag length Value) format.

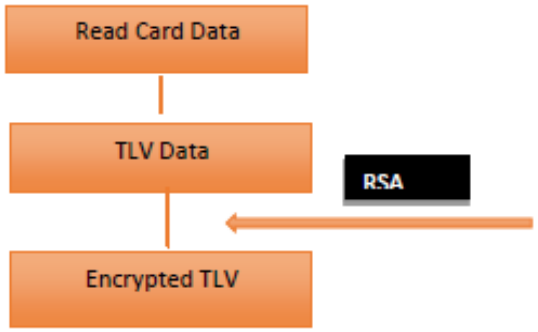

Figure 3: The data flow diagram

- TLV data is data representation in EMV specification, itself is in encoded form.
- RSA algorithm applied over TLV data encrypts the data and makes the personal data of the credit or Debit Card data secure.
- The encrypted data is sent over the Acquirer.
- Asymmetric Algorithms likes and ADSA can also be used to obtain the secured data.
- Data security as well as Hardware security can also be achieved.

EXPERIMENT DISCUSSION

Data analysis

About EMV Tags and it working explained using ReadCardData.ReadCardData module reads the data from the payment cards and returns the data in TLV format. Tag Length and value.

Table 1: Data Returned by the Read Card Module is Explained in Below Table

Tag Identifier	Description
5F20	Cardholder Name
57	Track 2 Equivalent Primary Account Number Expiration Date (YYMM) Service Code
5A	Cardholders account number
5F24	Date of Expiry

For Example,

1.5A085413330089601075

Where, 5A: tag name two characters, 08: length in bytes, 5413330089601075 – tag value in HEX format.

(16 characters)There some special tags with 'F' that is two characters, such as "4F".

IMPLEMENTATION RESULT

RSA algorithm applied over TLV data encrypts the data into hexadecimal formats as shown in Figure 4.

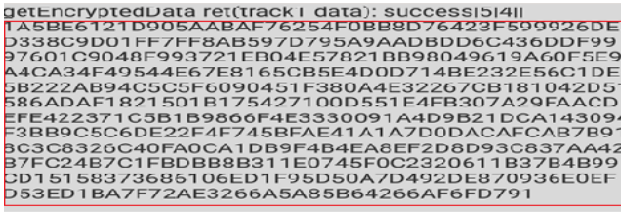

Figure 4: Snapshot of the secure data after encryption

CONCLUSION

- EMV read data even though is in encoded TLV format, this alone won't be enough to eliminate credit card fraud.
- Security can be achieved layer by layer and EMV system is prone to specific.
- Encryption could be used at PED level as well at application level. The encrypted data is sent to the issuer.
- Using the right kind of encryption and with authentication using tokens perhaps we can eliminate the EMV frauds from the system.

Acknowledgment

I would like to acknowledge the guidance I received during this project from Associate Professor, Meenakshi. Sundaram Department of CS& E, RIT, Bengaluru.

REFERENCES

1. Security Protocols and Evidence: Where Many Payment Systems Fail.By Steven J. Murdoch, Ross Anderson. Financial Cryptography and Data Security, Barbados, 03–07 March 2014.
2. Chip and Skim: cloning EMV cards with the pre-play attack.By Mike Bond, Omar Choudhry, Steven J. Murdoch, Sergei Skorobogatov, Ross AndersonIEEE Symposium on Security and Privacy, San Jose, CA, US, 18–21 May 2014.
3. EMV Is No Payment Security Panacea.Implement EMV and you eliminate payment card fraud, right? Wrong.By Jeff Goldmen| Posted January 16, 2015.
4. Common Payment Application Specification *Version 1.0 December 2005.*
5. Anderson, R.: Offender tagging. Light Blue Touchpaper (September2013), http://www.lightbluetouchpaper.
6. Anderson, R., Bond, M., Murdoch, S.J.: Chip and spin. Computer Security Journal 22(2) (2006), http://www.chipandspin.co.uk/spin.pdf 5. ARM: Building a secure system using TrustZone technology (April 2009),
7. Bellare, M., Yee, B.: Forward-security in private-key cryptography. In: Topics in Cryptology – CT-RSA 2003, LNCS, vol. 2612, pp. 1–18. Springer (2003).
8. Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S., Anderson, R.: Chip and skim: cloning EMV cards with the pre-play attack. In: Workshop on Cryptographic Hardware and Embedded Systems (CHES). Leuven, Belgium (September 2012), (invited talk) arXiv: 1209.2531.
9. Clayton, R., Bond, and M.: Experience using a low-cost FPGA design to crack DES keys. In: Workshop on Cryptographic Hardware and Embedded Systems (CHES). LNCS, vol. 2523, pp. 579–592. Springer-Verlag, London, UK (2002),
10. Drimer, S., Murdoch, S.J.: Keep your enemies close: Distance bounding against smartcard relay attacks. In: USENIX Security Symposium (August 2007) 10. EMVCo: About EMV, http://www.emvco.com/about_emv.aspx.