Problems with CBC Block Encryption for PANs

Ashok Misra

ashok@misraonline.com

Abstract

- Permanant Account Number (PAN) encryption in an ecommerce merchant databases presents unique application issues.
- Block encryption primitives using Cipher Block Chaining (CBC) mode preclude the possibility of supporting an efficient lookup functionality.
- Since CBC encryption mode is not idempotent [1] one way hashes for PANs are needed in order to support lookup.
- The payment community does *not* view a one way hash of a PAN as a security violation. Ironicaly, its use is recommended by PCI DSS best practices.
- On the other hand, security experts categorically proscribe the use of an idempotent block cipher implementation such as Electronic Code Book (ECB).
- Storage of SHA1 hashes for payment information follows best practise, PCI guidelines and buzzword compliance.
- This paper presents a minority opinion and argues that security is weakened dramatically by employing one way cryptographic primitives for PANs in order to support lookup.

Introduction

The primary purpose of encrypting a PAN in a merchant ecommerce database is to safeguard against an maleficent intruder gaining access to the raw PAN.

The entire asset being protected in credit card environments is typically a 16 byte string. Key attributes that are connected with the PAN i.e. expiry date, brand, last four digits are declassified for valid reasons.

For most acquirer processing systems, the only valid Credit Card atribute required in order to secure an authorization on an instrument is the PAN. Other related fields such as Billing Address, CVV, Expiry date, etc are not mandatory fields for authorizations.

Message Integrity with the encryption scheme for the PAN field in isolation is not a requirement. The PAN is never the sole field in a financial message payload. If Alice knows the cipher text of her PAN in a particular merchants database, that knowledge does not compromise security. Security is achieved on the strength of the cryptographic algorithm and the key management employed.

Message integrity is a strong requirement when financial messages containing PANs are transported. However as mentioned, the PAN is merely a field in the payload of the financial message being transported. Financial messages are in fact transported either using a symmetric key for a block cypher in CBC mode or by using some form of Public Key Encryption.

The use of a block cipher in CBC mode for a financial message payload is *NOT* being questioned in this paper. Indeed, there are very sound reasons for using CBC mode for the transport of financial message payloads.

This paper questions the use of a block cipher in CBC mode for encrypting PANs where the aforementioned primitive necessitates the employment of a one way, algorithmically non reversible function in order to support a lookup functionality.

Typical PAN Security Implementation

A typical encryption design for PANs is as follows:-

1. In order to encrypt a PAN, a hardware device uses entropy to generate a unique Initialaztion Vector (IV). A Block Cipher Algorithm uses the IV and a cryptographic symmetric key to produce cypertext in CBC mode. The IV that was used is concatenated with the cipher text and persisted in a database.
2. The customers billing information record associated with the payment instrument is linked with the cipher text from the previous step.
3. When a payment application needs to charge a customer, it picks up cipher text linked with the customer record, chomps the IV out of the cipher text and uses that as input with the cipher text to the decrypt function (which has access to the symmetric block cipher key).
4. Payload for the application message to the financial institution is built in accordance with the destination institutions message protocol, using the clear text instrument.
5. Payload is encrypted under layer 7 and delivered to the financial institutions end point.

Requirements for Lookup

There are several valid use cases in ecommerce that require a lookup functionality. To cite a few :-

1. Visa Account Updater (VAU) enables the exchange of updated account information electronically among participating issuers, acquirers, and merchants that process account-on-file Visa transactions. Thus the VAU receving application at the ecommerce merchants end needs to be able to lookup the VAU record being updated in order to modify it.
2. Bob sees charge from an unrecognized merchant in his bill. No order number is stamped in the descriptor field. He calls up the merchant & disputes the charge.
3. A financial institution sends its merchant a list of cards on which recent fraud was reported. The Merchant needs to terminate the entitlements for customers using these cards.
4. Further, following the previous step, the merchant wants to blacklist the cards so their entry is blocked on front end order page.

The crypto design for CBC block encryption satisfies the requirements for the secure storage of payment instruments, however it does not support lookup.

In order to extend lookup, financial applications must support a method that accepts a clear test PAN and returns the pointer to the encrypted record. A non idempotent CBC encryption implementation precludes the design from achieving this functionality easily. The only way to 'lookup' is by recursively traversing through the entire database of persisted encrypted values, invoking the decrypt on each row and comparing the result with the the value to be looked up. This is clearly computationally intensive and not a scalable approach.

In order to reliably support a lookup functionality with a non idempotent block cipher mode, a one way hash of the PAN is computed, associated with the customer billing record and persisted in a discrete field.

PAN Characteristics

A PAN fundamentally possesses extremely low entropy. The reasons for this are as follows:-

1. Most Bankcards (Visa & MC) are typically 16 bytes wide. AMEX is typically 15 bytes.
2. Valid PANs are numeric only and must pass the luhn algorithm.
3. Subcript 0 to 6 represents the issuing bank bin. There are near exhaustive lists for valid bins.
4. Brand (visa, MC, Amex) can be derived from the first byte of a PAN.
5. Tail (last 4 or 5 digits) is declassified for printing on receipt or proforma.

It can be seen from the above that a PAN is patently poor candidate to be subjected to a one way algorithm.

It is not a non trivial operation to build a rainbow table of valid PANs to one way hashes tuples.

This brings up the need for physical security of back up tapes (if they are copied to backup media without any further encryption). Further, Physical transport and off site storage of the back up tapes would similarly present a security issue. Had the billing database contained cipher text only, offsite issues would be moot.

Conclusions

Security drops dramatically by using a one way hash to support lookup for PANs.

If the block cipher algorithm used were to be implemented in an idempotent manner (using ECB instead of CBC) a hash on PAN would be unnecessary as lookup could be implemented by overloading the encrypt method.

Ironicaly, most cryptography papers written by leading experts summarily caution against using ECB mode for block ciphers. This encryption mode is usually discussed as an academic exercise, in order to highlight its vulnerabilities. This prescriptive advice is incongruent for the application environment arounds PANs.

Security is undeniably only as good as the weakest link. There is questionable overall security gain in employing the use of a cryptographically strong block cipher algorithm using the full entropy of the symmetric key and then weakening its implementation with a one way hash of the asset being protected.

EBC mode for block ciphers clearly has some well documented drawbacks.Its use is generally questionable for raw payloads larger than one block. However, these drawbacks do not manifest themselfs when this primitive is used specifically for PAN encryption.

Overall security is weakened considerably by employing the use of a non idempotent encryption design that necessities the storage of a one way hash in order to support a lookup functionality.

References

1. PCI DSS 1.1 https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
2. Payment Application Best Practices
   usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc
3. Practical Cryptography - Niels Ferguson ISBN-10: 0471223573
4. Applied Cryptography:Protocols Bruce Schneier ISBN-13: 978-0471117094

Notes

1. It is assumed that a random Initialation Vector or nonce is used. CBC mode would be idempotent if a global site wide nonce were used, but that would defeat the purpose of CBC.