black hat®
USA 2016

Samsung Pay:

Tokenized Numbers, Flaws and Issues

Salvador Mendoza

Twitter: @Netxing

Salvador_m_g@msn.com

About Me

Salvador Mendoza

- Researcher
    - Android apps and tokenization mechanisms.
- College student
    - A. S. Computer Science Degree
    - Computer Network Administration Certificate
    - Computer Programming Specialist Certificate

Agenda

- Terminology
- Tokenized numbers
- Numbers and analyzing a token
- MST and NFC protocols
- Fragile tokenized process and storage
- Possible attacks
- JamPay tool

Terminology

- NFC: Near Field Communication
- MST: Magnetic Secure Transmission
- VST: Visa Token Service
- Tokenized numbers: A process where the primary account number (PAN) is replaced with a surrogate value = Token.
- Token: An authorized voucher to interchange for goods or service.
- TSP: Token Service Provider
- PAN: Primary Account Number

Analyzing Tokenized Numbers (Token)

%4012300001234567^21041010647020079616?;

4012300001234567^21041010647020079616?

~4012300001234567^21041010647020079616?

% = Start sentinel for first track

^ = Separator

? = End sentinel for every track

; = Start sentinel for second track

~ = Start sentinel for third track

A tokenized number follows exactly the same format of IATA/ABA; emulating perfectly a swiping physical card.

Analyzing a Track

Second track ;4012300001234567^2104101064702007961 6?

The first 16 digits are the new assigned CC number: 4012300001234567

401230-000-1234567	401230	000	01234567
New CC number	Private BIN #	Never change, from original CC	Still researching

Analyzing a Track

Second track = ;4012300001234567^21041010647020079616?

The last 20 digits are the token's heart: 21041010647020079616

2104-101- 0647020079616	21/04	101	064702-0079-616
Token's heart.	New expiration date.	Service code: 1: Available for international interchange. 0: Transactions are authorized following the normal rules. 1: No restrictions.	064702: It handles transaction's range/CVV role. 0079: Transaction's id, increase +1 in each transaction. 616: Random numbers, to fill IATA/ABA format, generated from a cryptogram/array method.

NFC/MST offline/online mode

Without internet; did not change the middle counter

%4012300001234567^21041010**82000(constant)**0216242?

%4012300001234567^21041010**82000**0217826?

%4012300001234567^21041010**82000**0218380?

[…]

With internet, the middle counter increased +1:

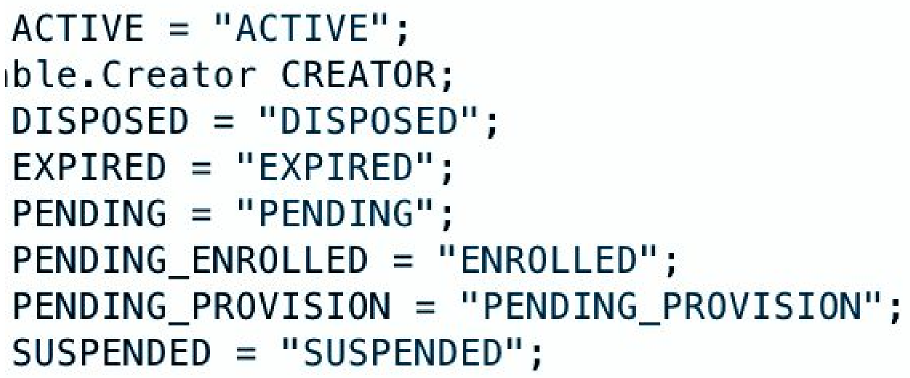
%4012300001234567^21041010**82000**0233969? %

4012300001234567^21041010**82000**0234196?

%4012300001234567^21041010**82001**0235585? ← **+1**

Token Phases

- Active: Normal status after generated.
- Pending: Waiting for TSP’s response.
- Disposed: Destroyed token.
- Enrolled: Registered token.
- Expired: Became invalid after period of time.
- Suspended_provision: Valid PAN, requesting more info.
- Suspended: VST will decline the transaction with a suspended token.



```
ACTIVE = "ACTIVE";
ble.Creator CREATOR;
DISPOSED = "DISPOSED";
EXPIRED = "EXPIRED";
PENDING = "PENDING";
PENDING_ENROLLED = "ENROLLED";
PENDING_PROVISION = "PENDING_PROVISION";
SUSPENDED = "SUSPENDED";
```

Updating Token Status

```
//SAMPLE REQUEST URL
https://sandbox.api.visa.com/vts/provisionedTokens/{vProvisionedTokenID}
/suspend?apikey={apikey}
// Header
content-type: application/jsonx-pay-token: {generated from request data}
// Body
{
  "updateReason": {
    "reasonCode": "CUSTOMER_CONFIRMED",
    "reasonDesc": "Customer called"
  }
}
// SAMPLE RESPONSE
// Body
{}
```

Source: Visa Developer Center

Files Structure

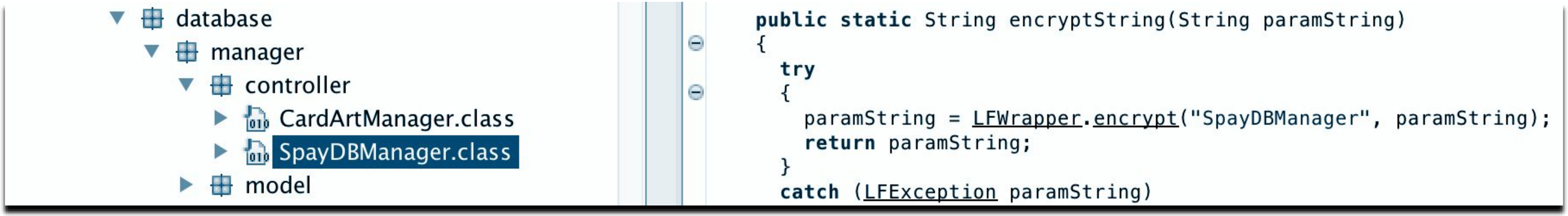
Databases > 20	Directories/files
vasdata.db, suggestions.db, mc_enc.db	/system/csc/sales_code.dat, SPayLogs/
spay.db, spayEuFw.db, PlccCardData_enc.db	B1.dat, B2.dat, pf.log, /dev/mst_ctrl
membership.db, image_disk_cache.db, loyaltyData.db	/efs/prov_data/plcc_pay/plcc_pay_enc.dat
transit.db, GiftCardData.db, personalcard.db	/efs/prov_data/plcc_pay/plcc_pay_sign.dat
CERT.db, MyAddressInfoDB.db, serverCertData.db	/sdcard/dstk/conf/rootcaoper.der
gtm_urls.db, statistics.db, mc_enc.db	/efs/pfw_data, /efs/prov_data/pfw_data
spayfw_enc.db, collector_enc.db, **cbp_jan_enc.db**	/sys/class/mstldo/mst_drv/transmit… many more

cbp_jan_enc.db

CREATE TABLE tbl_enhanced_token_info (_id INTEGER PRIMARY KEY AUTOINCREMENT, **vPanEnrollmentID** TEXT, **vProvisionedTokenID** TEXT, token_requester_id TEXT, encryption_metadata TEXT, tokenStatus TEXT, payment_instrument_last4 TEXT, payment_instrument_expiration_month TEXT, payment_instrument_expiration_year TEXT, token_expirationDate_month TEXT, token_expirationDate_year TEXT, **appPrgrmID** TEXT, static_params …

https://sandbox.api.visa.com/vts/provisionedTokens/**{vProvisionedTokenID}**/suspend?apikey=**{apikey**}

Flaws and Issues



```
public static String encryptString(String paramString)
{
  try
  {
    paramString = LFWrapper.encrypt("SpayDBManager", paramString);
    return paramString;
  }
  catch (LFException paramString)
```

- paramString = **LFWrapper.encrypt("OverseaMstSeq", paramString);**
- bool1 = b.edit().putString(paramString, **LFWrapper.encrypt ("PropertyUtil"**, null)).commit();
- String str = **LFWrapper.encrypt("tui_lfw_seed", Integer.toString (paramInt));**

Flaws and Issues

- Token expiration date is in blank.
- ivdRetryExpiryTime implements timestamp format.

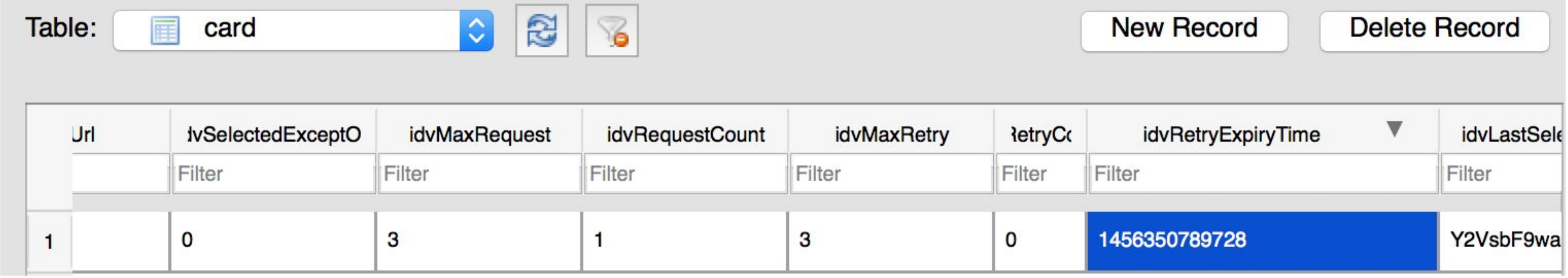


Table: card

	Url	ivSelectedExceptO	idvMaxRequest	idvRequestCount	idvMaxRetry	RetryCc	idvRetryExpiryTime ▼	idvLastSele
		Filter	Filter	Filter	Filter	Filter	Filter	Filter
1		0	3	1	3	0	1456350789728	Y2VsbF9wa

- **If Samsung Pay generated a token, but it is not used to make a purchase, that token still active/alive.**

Attacks

Different scenarios:

- Social engineering (Video)
- Jamming MST signal (video/tool)
- Reversing the encrypt/decrypt function
- Guessing the next token

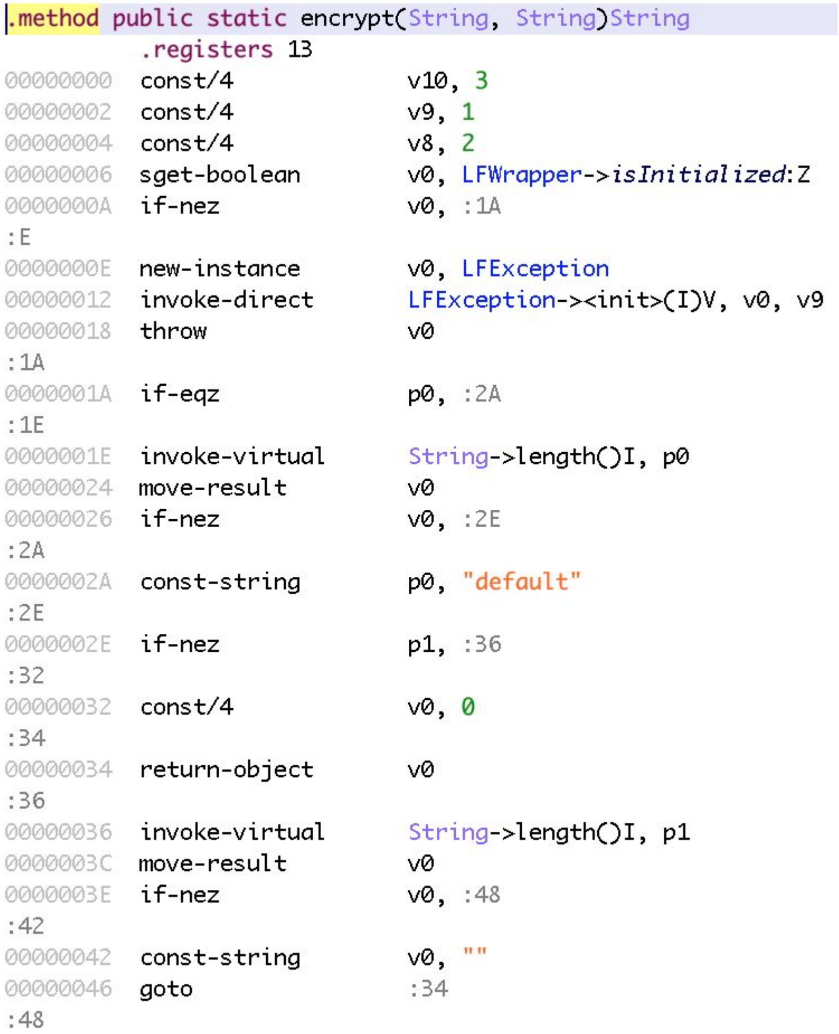
Social Engineering

https://www.youtube.com/watch?v=QMR2JiH_ymU

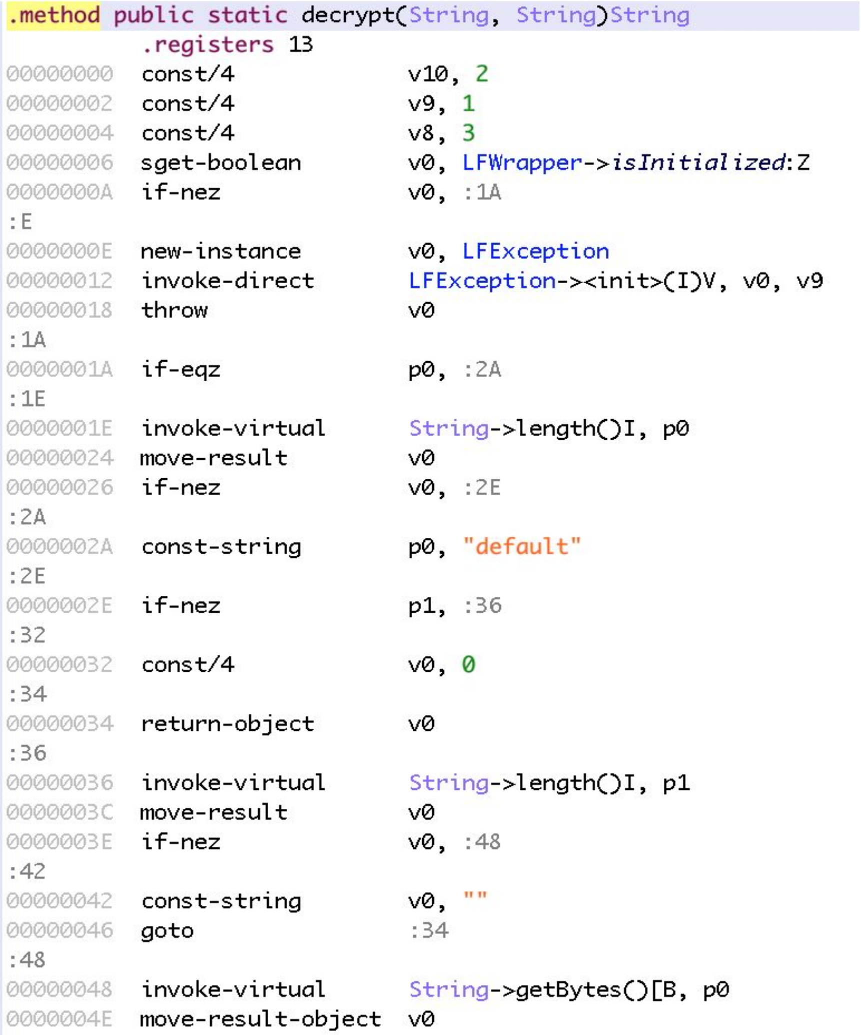
JamPay

https://www.youtube.com/watch?v=CujkEaemdyE

Encrypt/Decrypt Functions



```
.method public static encrypt(String, String)String
                .registers 13
00000000   const/4              v10, 3
00000002   const/4              v9, 1
00000004   const/4              v8, 2
00000006   sget-boolean         v0, LFWrapper->isInitialized:Z
0000000A   if-nez               v0, :1A
:E
0000000E   new-instance         v0, LFException
00000012   invoke-direct        LFException-><init>(I)V, v0, v9
00000018   throw                v0
:1A
0000001A   if-eqz               p0, :2A
:1E
0000001E   invoke-virtual       String->length()I, p0
00000024   move-result          v0
00000026   if-nez               v0, :2E
:2A
0000002A   const-string         p0, "default"
:2E
0000002E   if-nez               p1, :36
:32
00000032   const/4              v0, 0
:34
00000034   return-object        v0
:36
00000036   invoke-virtual       String->length()I, p1
0000003C   move-result          v0
0000003E   if-nez               v0, :48
:42
00000042   const-string         v0, ""
00000046   goto                 :34
:48
```



```
.method public static decrypt(String, String)String
                .registers 13
00000000   const/4              v10, 2
00000002   const/4              v9, 1
00000004   const/4              v8, 3
00000006   sget-boolean         v0, LFWrapper->isInitialized:Z
0000000A   if-nez               v0, :1A
:E
0000000E   new-instance         v0, LFException
00000012   invoke-direct        LFException-><init>(I)V, v0, v9
00000018   throw                v0
:1A
0000001A   if-eqz               p0, :2A
:1E
0000001E   invoke-virtual       String->length()I, p0
00000024   move-result          v0
00000026   if-nez               v0, :2E
:2A
0000002A   const-string         p0, "default"
:2E
0000002E   if-nez               p1, :36
:32
00000032   const/4              v0, 0
:34
00000034   return-object        v0
:36
00000036   invoke-virtual       String->length()I, p1
0000003C   move-result          v0
0000003E   if-nez               v0, :48
:42
00000042   const-string         v0, ""
00000046   goto                 :34
:48
00000048   invoke-virtual       String->getBytes()[B, p0
0000004E   move-result-object   v0
```

Guessing a Token?

Samsung Pay in Mexico?

https://www.youtube.com/watch?v=EphR18sSjgA

We did it first: Thanks @Sabasacustivo

Greetz, Hugs & Stuff

Samy Kamkar (@samykamkar)
Pedro Joaquin (@_hkm)
Andres Sabas (@Sabasacustico)
Luis Colunga (@sinnet3000)
RMHT (raza-mexicana.org)
The Extra’s mom

Questions?

Thank you!

Salvador Mendoza

Twitter: @Netxing

Salvador_m_g@msn.com

Black Hat Sound Bytes

- Samsung Pay has some levels of security, but it is a fact that could be a target for malicious attacks.

- Samsung Pay has some limitations in the tokenization process which could affect customers’ security.

- Finally, tokens generated by Samsung Pay could be used in another hardware.