Security in Mobile Payments: A Report on User Issues

March 2017

Abhipsa Pal
FPM student, Decision Sciences and Information Systems
IIM Bangalore
abhipsa.pal14@iimb.ernet.in

Sai Dattathrani
Manager, Centre for Software IT Management
IIM Bangalore
sai.dattathrani@iimb.ernet.in

Dr. Rahul Dé
Professor, Decision Sciences and Information Systems
IIM Bangalore
rahul@iimb.ernet.in

1 Introduction

With the rapid development of information technology, ubiquitous mobile phones, and the impact of the demonetization scheme of the Government of India, India has experienced a significant surge in the number of electronic transactions through mobile payment apps and services[1]. However, around the world, spread of electronic banking has resulted in thousands of cybercrimes and monetary thefts by cybercriminals[2]. The security risks related to electronic transactions through mobile payments are high due to various technological and other reasons[3]. In this study we focus on the risks associated with Indian mobile phone based payment systems. We conducted experiments with five popular mobile payment systems in four broad categories – wallets (PayTM, FreeCharge), direct link with user's bank (BHIM), specific bank's app for account holders (iMobile by ICICI Bank), and basic USSD service (dialing *99#). We developed six key security principles combining the Basel Committee's 'Risk Management Principles for Electronic Banking'[4] and the RBI norms for electronic banking transactions[5]. These six principles were used to evaluate the security concerns related to the payment systems. We found that all the above apps and services have security concerns based on one or more of the six principles. Even while we were conducting the study, we observed that the features of the apps and services were constantly evolving and changing. Hence, we would like to add the caveat that the evaluation of the apps in this report is as observed during our study conducted between December'16 and January'17, and it is highly likely that some of the concerns presented in this report have been addressed, and perhaps new concerns have emerged.

2 Study approach

This study was conducted largely on the campus of IIM Bangalore, with students, faculty and staff as subjects who engaged in mobile transactions. The study was conducted entirely in the months of December'16 and January'17. The study included evaluation of the apps installed on smartphones with various versions of Android OS, iOS in case of Apple devices, and basic mobile phones without data connection. The time spent with the subjects ranged from thirty to sixty minutes. A total of 75 activities, including installation, transactions, login/logout, were studied. The subjects were asked to share their experience as the experiment was in progress so that it could be recorded for further analysis. Additionally, the researchers participated in the transactions, when required. The apps chosen for each of the category of online payment were based on their popularity. They are as follows:

- *Category 1*: Mobile Wallets – PayTM, Freecharge
- *Category 2*: Apps linking to bank accounts – BHIM, PhonePe
- *Category 3*: Banks' Apps for Account Holders – iMobile (ICICI Bank)
- *Category 4*: Basic USSD using *99#

[1] The Indian Express, 30-Dec-2016
[2] Times of India, 10-Jan-2017
[3] Security Intelligence, 14-Feb-2017
[4] Basel Committee, 2003
[5] Reserve Bank of India, 2008

The apps were evaluated on the RBI guidelines[6] and BASEL norms[7] for secure digital financial transactions as below:

1. **Confidentiality**: The transaction, bank account details, and wallet balance of the user should be confidential and not accessible to unauthorized users or third-party vendors. To evaluate this aspect in the apps, we investigated whether the data (in-transit or saved data) was accessible only to intended stakeholders

(Adopted from Basel e-transaction Security Controls principle-10 and RBI guidelines' 1st property)

2. **Transaction non-repudiation management**: In the case of mobile payments, transactions are confirmed using notifications, SMS and emails containing essential details (amount, time of transaction, sender, receiver, app vendor name and comments) and confirmation of the transaction to both sender and receiver, and these ought to be logged and tracked to prevent false denial. To evaluate this aspect, we investigated whether
    a. The transaction logs were maintained and if the data in the logs could be used in case of transaction repudiation
    b. The app tracked and warned in cases of unusual transaction patterns – for example, multiple transactions being carried out in quick succession (within a few seconds)

(Adopted from RBI guideline's 4th property)

3. **Authentication of the identity of the customers**: It is very important for mobile apps, during a transaction, to ensure that it is the authenticated account holder who is transferring the money. Authentication can be achieved by the use of unique passwords or biometrics of the user. To evaluate this aspect, we investigated
    a. Whether every transaction was authenticated, and conducted with explicit consent
    b. The strength of login and logout process authentication. If this process is not sufficiently authenticated, it would be similar to leaving the door open for any intruder to enter the house at any time.

(Adopted from Basel e-transaction Security Control principle-4 and RBI guideline's 3rd property)

4. **Data and transaction integrity**: The transaction details and wallet amounts shown to the customers in app notifications and statements should be consistent with actual details. To evaluate this aspect, we investigated whether the
    a. Data maintained and displayed were accurate and consistent
    b. Transaction confirmation processes followed the norms of a reliable and consistent transaction

(Adopted from Basel e-transaction Security Control principle-8 and RBI guideline's 2nd property)

[6]'Mobile Payments in India - Operative Guidelines for Banks' was issued by the Reserve Bank of India in 2008 for promoting secured mobile transactions by ensuring four properties: (1)confidentiality (2)integrity (3)authenticity and (4)non-repudiability.

[7]The Basel Committee on Banking Supervision identifies the major risks associated with electronic banking and digital transactions, and develops a set of principles that should be followed by the banking institutions and other electronic payment systems in order to control and reduce the risks associated.

5. **Access and availability**: In case of mobile payment services, the network forms a key feature for the availability of the services to the customer. Some apps and USSD systems work through SMS or voice calls from the mobile phone, thus being available to customers who do not have internet or data connections on their mobile devices. To evaluate this aspect, we investigated the
    a. Variety of modes in which the services were available
    b. Reliability of the service (such as availability of information on ombudsman, security and more)

(Adopted from Basel e-transaction Legal and Reputational Risk Management principle-13)

6. **Privacy of customer information**: The payment app or service should not ask for customer data that violates privacy or increases risk of identity theft. This principle is particularly prominent during app installation when the user needs to give access permissions to the app for a multiple number of fields. To evaluate this aspect, we investigated whether the requested privileges were justified (whether the functionality of the app could be compromised without access to the privileges).

(Adopted from Basel e-transaction Legal and Reputational Risk Management principle-12)

Findings from the study

Legend: A blue box indicates passing the evaluation test; A gray box indicates not satisfying in all the cases; A red box indicates a security violation.

Paytm evaluation

Confidentiality	Transaction Repudiation Management	Authentication	Data and Transaction Integrity	Access & Availability	Customer Privacy Requirements
During a bank-to-wallet money transfer, the bank issues an OTP. Paytm accesses this particular OTP through its own popup. The OTP is generated by the bank for the transfer, and is not meant for Paytm.	Unusual transaction patterns though logged, they are not detected and no warning is provided to the user. Will be an issue in case of fraud transaction repudiations.	Certain mobile phones such as Apple iOS and the latest version of Android allow fingerprint identification to be setup for every transaction.	Each transaction is identified by a unique Transaction ID, which gives a sense of transparency and accountability.	Details on transaction limits & FAQs on security / ombudsman aspects are difficult to find.	Users have concerns with Paytm requiring privileges such as access to identity, media, camera, even though these may not be required for the current transaction.
The SMS and email notifications are accessible to anyone who has access to the phone.		Vendors like Uber and BigBasket automatically deduct the amounts without explicit consent.	Easily readable monthly statement provides for transaction accountability. This is sent over email.	Money transfer available without internet through phone call and secured Paytm PIN.	

		Some of the concerns with login / logout processes are as below: User is perpetually logged in and no password is required for any transaction. Paytm never logs out the user automatically. It is not easy to find the logout option. The app does not have a session timeout. These shortcomings could allow fraudulent transactions to occur, if the user is not careful.	Accurate data such as available balance, monthly usage data is not always available. Some inconsistencies were observed during our study.		
			Transaction confirmation SMS & email are provided immediately in line with reliable transaction procedures.		

Notes from the evaluation:

- When money is transferred from bank to wallet, the bank sends an OTP to complete the transaction. This is generated by the bank, and is to be entered in the bank's portal. However, Paytm picks up the OTP message, when it is not intended for Paytm. Some of our subjects expressed concern over this violation of data confidentiality.

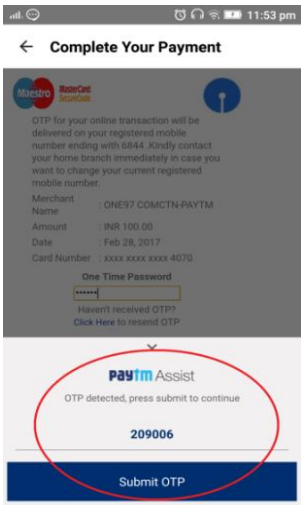

Figure: Paytm popup accesses OTP generated by user's bank.

- Allows for vendors such as Uber, Bigbasket to not only be able to view the users' available balance, but also allows for automatic deduction without the explicit consent of the user.

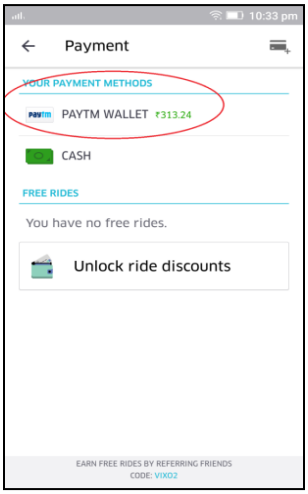

Figure: Uber accessing user's Paytm wallet balance data.

Freecharge evaluation

Confidentiality	Transaction Repudiation Management	Authentication	Data and Transaction Integrity	Access & Availability	Customer Privacy Requirements
The SMS and email notification is accessible to anyone who has access to the phone.	Unusual transaction patterns, though logged, are not detected and no warning is provided to the user. Will be an issue in case of fraud transaction repudiations.	Not linked to vendors, hence there is no concern of deducting money without explicit consent.	The balance amount does not accurately reflect the available transaction amount.	Does not work without internet. No option for conducting transactions using phone calls.	Though the app explicitly requests for privileges, it does not allow transactions without access to phone, SMS and storage.
		Some of the concerns with login / logout processes are as below: User is perpetually logged in and no password is required for any transaction. FreeCharge never logs out the user automatically. It is not easy to find the logout option. There is no session timeout in the app. It allows for autologin to the app. Transaction is not password-protected. These shortcomings could allow fraudulent transactions to occur, if the user is not careful.	Each transaction is identified by a unique Transaction ID, which gives a sense of transparency and accountability. Transaction confirmation SMS & email are provided immediately in line with reliable transaction procedures.	Details on transaction limits & FAQs are available.	

		There is no mechanism (such as authentication using fingerprint) to secure every transaction.	Monthly statement not sent over email, but can be checked under the 'My Transactions' tab.	Details on ombudsman aspects are difficult to find.	

Notes from the evaluation:

- The FreeCharge wallet balance displayed in the home page of a user did not represent the transferable balance accurately. On clicking on it, a pop-up displayed that the amount was not usable cash balance but voucher balance. Voucher balance is not transferable and usable only for paying to certain third party vendors like mobile recharge, movie ticket booking, etc. However, the wallet balance display was misleading, giving a sense of available cash balance. See figure-9a and b.

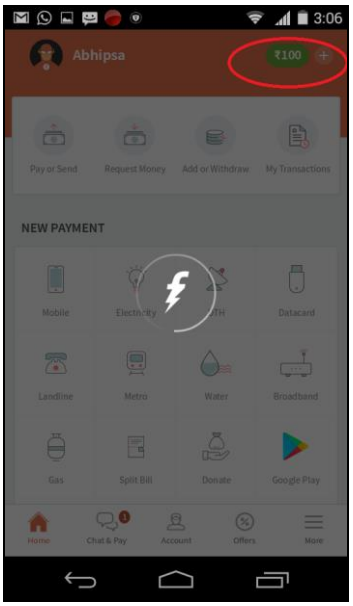

Figure 9a: FreeCharge wallet balance incorrectly shown as Rs.100 (which is unusable)

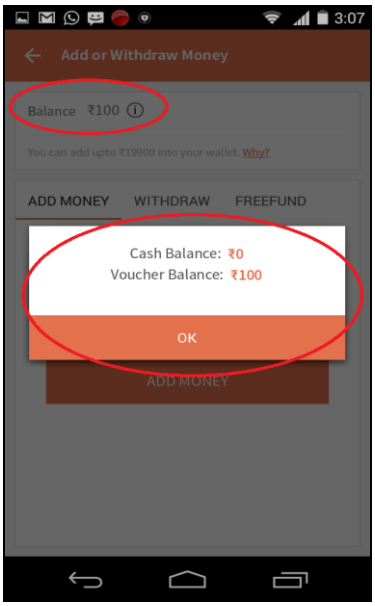

Figure 9b: On clicking on the FreeCharge wallet balance, shows voucher balance and cash balance separately

- In the latest Android and iOS platforms, FreeCharge allows users to explicitly accept or deny access to privileges. However denying access to phone, SMS and storage caused installation failure and did not allow the user to carry out any transaction. Refer to figure.

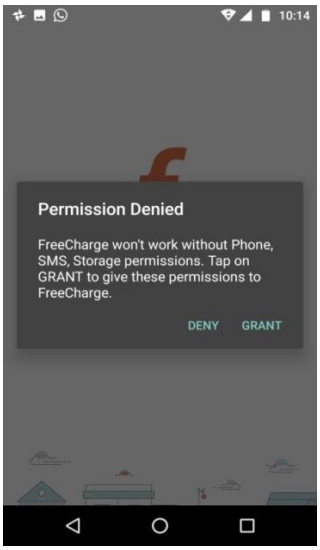

Figure 12: FreeCharge installation failed when user's Phone and SMS access permission was denied.

iMobile evaluation

Confidentiality	Transaction Repudiation Management	Authentication	Data and Transaction Integrity	Access & Availability	Customer Privacy Requirements
The SMS and email notifications (if and when sent by the bank) are accessible to anyone who has access to the phone.	The app offers generation of mini-statement of ICICI bank account of the user, but does not have separate passbook for app specific transactions.	App allows new app specific 4-digit-pin or allows for using the existing Internet Banking password.	The app never sends SMS/email confirmation for any transaction (but the bank may send a notification based on the users' preferences).	ICICI Bank's Instant Voice Response Banking is a service available via phone call. This is not an iMobile feature but since the app is only for ICICI bank accounts, the IVR service is sufficient for non-internet users.	Users have concerns with iMobile requiring privileges such as access to identity, media, camera, even though these may not be required for the current transaction.
The bank statement that is sent over email is locked with a password.		The app has an autologout / session timeout feature.	The monthly statement can be generated from the app. The bank sends the statement to the user. The accuracy concerns are hence non-existent.	The ombudsman and transaction repudiation process is well detailed and easily available at http://upiappindia.in/icici-bank-upi-complaint-box/.	

		The payee has to be added as a beneficiary before the payment is made.	.		
		If the payee has already been added and is in the list, it then allows for transactions to be carried out without a password.			

Notes from the evaluation:

- During the app installation and setup on the user's mobile device, the app asks the user to setup the password which will later be required by the user for app login. User selects one of the two options: existing internet banking password, or setting up a new 4-digit-pin. See figure.

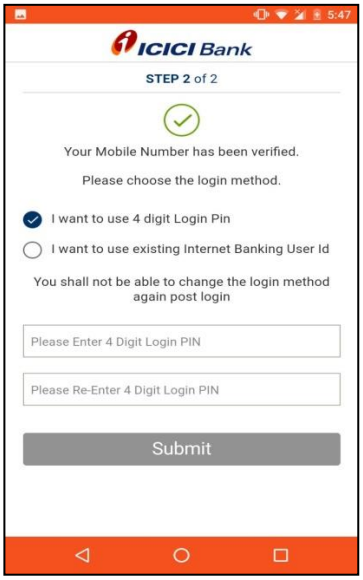

Figure 6: iMobile app login password setup.

- The app is directly linked to the user's ICICI bank account. The bank sends transaction notifications to users based on user preferences setup with the bank. However, the app does not send any notification (SMS or email) to the user. Since the app is managing the bank account separately, it should generate and send notifications to users to ensure transaction integrity and prevent non-repudiation.

BHIM evaluation

Confidentiality	Transaction Repudiation management	Authentication	Data and Transaction Integrity	Access & Availability	Customer Privacy Requirements
The SMS and email notifications (if sent by the bank, not BHIM) are accessible to anyone who has access to the phone.	Unusual transaction patterns, though logged, are not detected and no warning is provided to the user. This will be an issue in case of fraud transaction repudiations.	Password (4-digit-UPI pin) is needed for every transaction, and app login.	Time taken for transaction confirmation notification is very high (2 mins) in the case of successful transactions. In the case of a failed transaction, the time taken was almost 10 hours.	The app is USSD-based, hence does not need internet access.	Users have concerns with BHIM requiring privileges such as access to identity, media, camera, even though these may not be required for the current transaction.
The transaction history is accessible only if the person has a UPI pin.		The app has an autologout / session timeout feature.	Error messages are unclear to the users, which could be an issue in case of transaction repudiation.	Details on transaction limits and failures are available. However, ombudsman details are not available.	
		The app shows only UPI id of the payee, not the name, which may be confusing to merchants with many customers.	Notifications / alerts are sent by the app. But SMS / email notifications are sent by the bank (as per the standing instructions given by the bank account holder) and not the app.		

Notes from the evaluation:

- The transaction notifications for BHIM show only the UPI id of the payee, not her name. This may create confusion if the payee is one of the many customers transferring money to the same vendor.

- Logout is automated in BHIM. The user is logged out of her account when she exits from the app or after fixed time intervals. If the user has to access the app, she has to login using the previously setup 4-digit-PIN. See figure below.

Figure 7: BHIM login PIN.

USSD evaluation

Confidentiality	Transaction Repudiation Management	Authentication	Data and Transaction Integrity	Access & Availability	Customer Privacy Requirements
Needs UPI PIN for checking balance hence someone who has an access to phone cannot check balance.	Mini statement option available to check bank account transactions.	Needs UPI password even when beneficiary is saved.	For some users the *99# screen disappeared after some interval of inactivity, and then the user has to start from the beginning.	Does not need internet.	Asks for user's bank account number during NUUP registration. Does not ask for other privileges such as access to identity, media etc.
The SMS and email notifications are accessible to anyone who has access to the phone.		Joint account holder not notified.	Error messages are generic and unclear to the user.	Not possible to go to previous screen.	
				Deducts SMS cost from phone balance.	

				The RBI operative guidelines for mobile banking covers USSD based transactions, including ombudsman and other regulations / governance.	

Notes from the evaluation:

- The user may add a beneficiary in the app. However, even if the beneficiary has been added, every transaction from the user's bank account to the beneficiary's account requires the user to enter his/her UPI password.
- USSD system transfers money directly from user's bank account. If the bank account has a joint account holder, the other account holder should also be notified in case of a transfer. But transfer through USSD does not deliver transaction notification to the joint account holder.
- For some users, the USSD screen disappeared after some interval of inactivity, and the user has to repeat the entire process from the beginning, starting with dialling *99#.

Conclusion

Potential for confidentiality breaches was a problem observed for all the mobile payment methods, except USSD. This risk is highest if the user loses or misplaces her/his mobile phone, and higher still if the phone is unlocked or unprotected. Unauthorized access to the phone can reveal all details about transactions made for Paytm, Freecharge, iMobile and Bhim. The Paytm app has an unusual and unreasonable access to the one-time-password sent by a partner bank.

The management of the transactions, for subsequent repudiation, if needed, was inadequate for all the payment methods. There was no evidence of systematic analysis of transaction patterns with a warning to users of unusual or problematic transactions. For instance, if multiple, repetitive transactions are made in a very short period of time, this is not flagged by the payment systems. The lack of this feature is potentially harmful.

Authentication processes are enabled in the apps, however we found that there are security concerns. As with confidentiality issues, these security concerns arise if the user's phone is compromised. Paytm allows partners such as BigBasket and Uber to automatically deduct amounts, without authentication by the user. Though this provides convenience, it also allows unauthorized deductions (which may be disputed later). Paytm and Freecharge do not log out the user automatically, and logging out is also not easy for a new user, whereas iMobile and Bhim automatically log out the user. This feature in the latter two apps provides additional security from unauthorized usage.

Data and transaction integrity was quite sound for most of the apps. USSD has some issues with the menu screen disappearing if there is a delay in responding. This is an assuring aspect of the payment apps. Some concerns are that Paytm does not update the balance amount immediately and Freecharge reflects an inaccurate amount.

USSD and Bhim can operate on a voice and sms-based phone connection, and do not need a data plan (internet access) as the other payment apps do. Hence they enable a wider access. These two services are also clear on how disputes can be resolved, through an ombudsman, though this is known only through searching for details on websites than through everyday transaction screens.

There are serious privacy concerns with all the services studied. All the apps demand access to private data of the user, on the phone, without providing a clear rationale as to why this is needed. If some access is denied by the user, for instance access to the camera and media, even when the QR mode of payment is not being used, the apps do not function. This was consistently flagged by our respondents. Many respondents were not willing to install PhonePe, an app that was prominently launched and widely advertised, owing to its direct access to bank accounts, and hence, could not be included in our study.

Recommendations

Improvements in terms of data integrity (accuracy of balance sheet, transaction confirmation and such), and confidentiality (ensuring that the data is accessible only to intended stakeholders) will enhance the trust of the users. Certain aspects that were considered serious violations, such as allowing a merchant to deduct without the explicit consent of the user, should be addressed with urgency. While the USSD apps and bank apps have a clear guidance on the processes required to approach an ombudsman, the e-wallets are lacking on this aspect. This needs due diligence from the app vendors and regulatory authorities of India.

We also observed that the security vulnerability is inversely proportional to the users' awareness of security threats, technology and features of the phone. While educating users is definitely an approach, it is recommended that the OS vendors and app vendors enforce basic security hygiene (such as enforcing phone password, login password, logout and such) as part of their design.

References

[1] Basel Committee, (2003). Risk management principles for electronic banking.

[2] Reserve Bank of India, June 2008: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/84979.pdf

[3] Security Intelligence, 14-Feb-2017: https://securityintelligence.com/indian-banking-customers-beware-hackers-have-an-eye-on-your-money/

[4] The Indian Express, 30-Dec-2016: http://indianexpress.com/article/india/bhim-app-narendra-modi-digi-dhan-mela-demonetisation-4452004/

[5] Times of India, 10-Jan-2017: http://timesofindia.indiatimes.com/city/hyderabad/80-of-cybercrime-unreported-complaints-up-after-note-ban/articleshow/56432504.cms