Security of Unified Payments Interface (UPI)

Project Report for INSE 6150: Security Evaluation Methodologies

Submitted to: Professor Jeremy Clark

Submitted by

Devina Shah
40238009

Yash Khosla
40232363

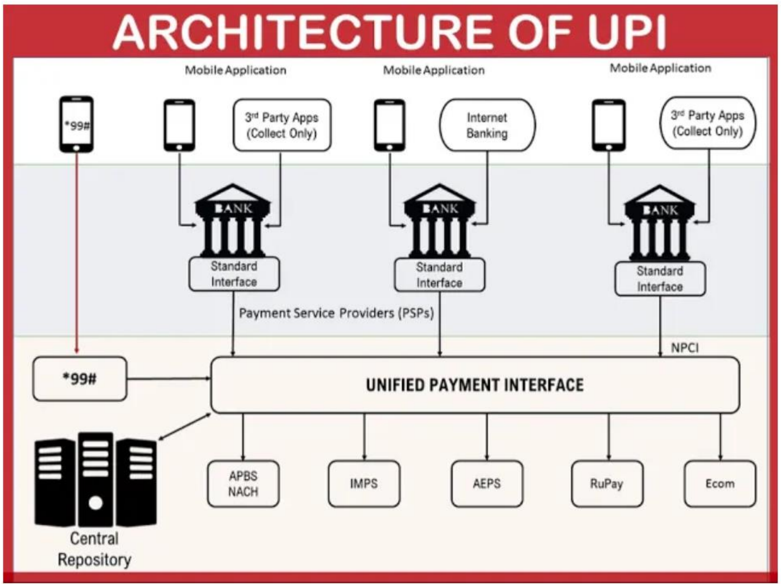
WHAT IS UPI

Unified Payments Interface (UPI) is an instant real-time payment system developed by National Payments Corporation of India (NPCI). The interface facilitates inter-bank peer-to-peer (P2P) and person-to-merchant (P2M) transactions through Virtual Payment Address, Cell Phone Number or QR Codes [1]. It powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood. UPI payment method is based on Immediate Payment Service (IMPS) which enables users to make payment 24*7 365 days.

UPI is a widely used payment system in India adopted by everyone from Small to Big Vendors and people of all age groups and literacy levels. The technology was widely used but saw a spike in transactions and users during COVID when cashless transactions was not only preferred but a requirement. The ease of UPI also enables users to pay securely to the vendors during delivery as well as carrying cash is not a requirement during in-store visits anymore. A smartphone that everybody carries anyway, enables users to make big payments through a click, after two-factor authentication. Such ease of transactions comes with some security risks which needs to be evaluated to improve the technology further, since it has been used so widely by millions of users, and deals with confidential user data.

In our study, we aim to do a comprehensive security evaluation of Unified Payments Interface using multiple evaluations methods which can be seen in the existing research for this state-of-the-art technology.

ARCHITECTURE AND WORKING OF UPI



UPI involves multiple layers of technology and security protocols to ensure seamless and secure fund transfer between bank accounts. As can be seen, the architecture has multiple components that we will discuss.

- User Interface – The payments are initiated by the user through their mobile application which can integrate multiple bank accounts. The user enters the receiver’s mobile number or Virtual Payment Address, the amount, followed by the pin of their App to authorise the payment.

- PSP (Payment Service Provider): The PSP is an intermediary between the mobile application and the UPI system. It is responsible for processing the transaction requests and ensuring the security of the transaction. PSPs can be banks or other entities authorized by the NPCI.

- National Payments Corporation of India (NPCI): The NPCI is the governing body that manages the UPI system. It facilitates communication between the banks, payment gateways, and IMPS to ensure that transactions are completed smoothly and securely.

- UPI System: The UPI system is the core of the UPI architecture. It serves as a centralized payment switch, routing the transaction requests between the PSPs and the banks.

- Banks: The banks hold the user's account details and process the transaction requests received from the UPI system. The banks also provide the necessary security measures to ensure the safety of the transaction.

- Security Protocols: UPI uses multiple layers of security protocols, such as two-factor authentication, biometric authentication, and encryption, to ensure that transactions are secure and cannot be intercepted or tampered with.

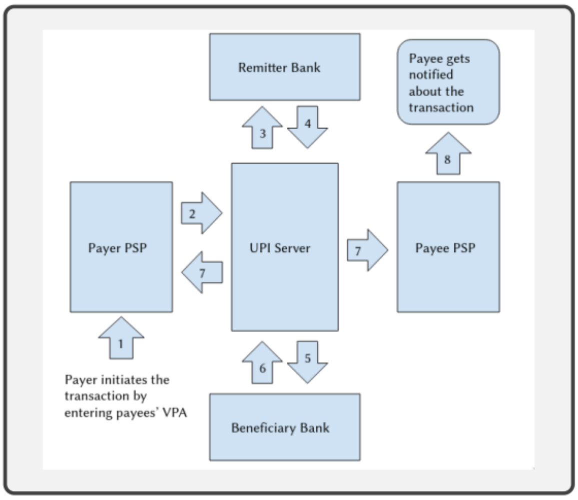
- Backend infrastructure: The backend infrastructure of UPI involves servers, databases, and other IT infrastructure that support the system's operations. Banks and payment gateways must have robust backend infrastructure to ensure that the system can handle a high volume of transactions and provide a seamless user experience.

Overall, the architecture of UPI is designed to be scalable, secure, and interoperable, enabling users to transfer funds between bank accounts instantly and seamlessly.

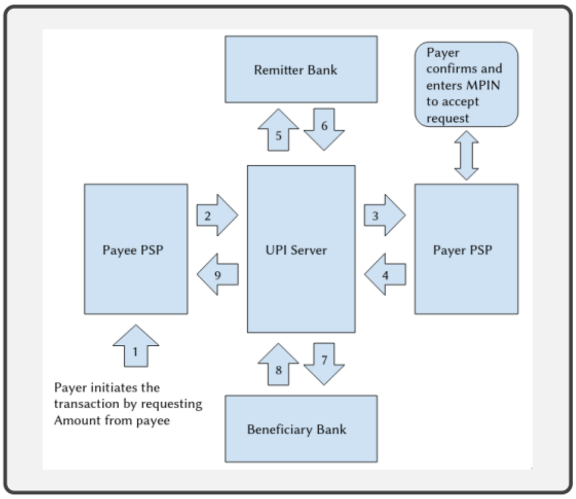
I. UPI allows two kinds of transaction – PUSH and PULL Transaction [2]

In PUSH transactions, the transaction is initiated by the payer when he enters the VPA address of the payee and then initiates the transaction by entering the amount and pin. Then the request is transferred to the UPI servers who look up the payer and the payee bank account in their database, and then it will debit the amount from the payer's account, and it will credit to the payee's account. This way, the transaction is completed, and the payer and payee are informed about the transaction. The full flow is explained in Fig below.

In a PULL transaction, the payee initiates the transaction by entering the VPA address of the payer. The PSP transfers the request to the UPI servers, which then transfers the request to the payer's PSP, and the payer receives a request for payment to the payee. He can either reject the request or accept the request. If he accepts the request, then enters his MPIN, the transaction will be processed, and after the amount is transferred successfully from the payer to the payee, the notification will be sent to both about the successful completion of the transaction; The flow is shown in Fig below.


Remitter Bank
Payee gets notified about the transaction
3
4
8
Payer PSP
2
7
UPI Server
7
Payee PSP
1
6
5
Payer initiates the transaction by entering payees' VPA
Beneficiary Bank

Push Transaction


Remitter Bank
Payer confirms and enters MPIN to accept request
5
6
Payee PSP
2
9
UPI Server
3
4
Payer PSP
1
8
7
Payer initiates the transaction by requesting Amount from payee
Beneficiary Bank

Pull Transaction

II. User Registration

A user can register for UPI service if they have a smart phone and a bank account. First, they have to install UPI PSP Apps from the respective app stores like Phone Pe, PAYTM, Google Pay, Etc. To connect the bank account to PSP app, enter the mobile number associated with it. It is used to send SMS containing device fingerprint (information containing the IMEI number, Device Id, App Id) for doing the first-factor authentication. This SMS is encrypted with PKI for security. During registration it will prompt the user to set the UPI pin. An OTP message will be sent to the user's registered phone number for verification. This serves as a second-factor authentication. User can also set up the screen lock for the App to increase the security. Finally, they have to choose a VPA for the account and then user have successfully registered for making transactions using UPI.

SECURITY EVALUATION OF UPI

The nature of our study interests' people in technical fields as well as people in finance and banking field. Hence, there are academic research papers on this subject that explores the technical side, such as effectiveness and security of the payment service providers (PSP) applications by reverse engineering the applications [4] [2]. Also, there are research papers that strictly focused on analysing the application through user reviews and evaluating how this technology and corresponding user behaviour pose a risk to its security. A research [5] conducted interviews with users on different hypothetical and real scenarios to understand the user's understanding of this state-of-the-art technology. [6] The security evaluation method used in this research entails analysing user review on google play for UPI applications. Another security evaluation method used [3] is by evaluating the different applications against RBI published guidelines. All these methods are comprehensive and effective in understanding the Security of Unified Payments Interface and contribute in enhancing their efficiency together.

I. Technical Evaluation of UPI: Reverse Engineering

The UPI Protocol details are not available to the people, and the researchers did not have access to UPI servers as well. Thus, they had to reverse-engineer the UPI protocol through the UPI apps that used it and had to bypass various security defenses of each app. [4] A careful examination was done on each stage of the UPI protocol to uncover the credentials required to progress in each stage, find alternate workflows for authentication, and discover leakage of user-specific attributes that could be useful at a later stage.

The following vulnerabilities were found which can be exploited further to attack the application. This has been discussed at length in the paper.

- One of the primary obstacles that attacker Eve must overcome to take control of Alice's account is UPI's device binding mechanism, which links Alice's phone number with her device. To bypass this, Eve needs to bind her phone with Alice's number, which is challenging due to the default workflow. However, an alternative workflow allows Eve to send Alice's cell number as an HTTPS message from her phone.

- The app also incorporates OTP verification for device binding. If Alice enters Bob's number on her phone, the UPI server sends the OTP to Bob's phone. If Bob shares the OTP with Alice, she can confirm it to the UPI server, binding her phone to Bob's number. Subsequently, Bob will receive all future SMS messages sent by the UPI server to Alice.

- In UPI's default workflow, Alice does not provide any secret shared with her bank to confirm her identity. Nevertheless, the UPI server discloses account details of an existing user, Alice.

[4][2] The researchers conducted a comprehensive security analysis of popular UPI apps and identified several security vulnerabilities, including inadequate server-side validation, insecure communication channels, and weak user authentication mechanisms. They also found that UPI apps often collect excessive amounts of personal data, which could be misused by malicious actors.

II. User Study of UPI: Interviews and User Review Analysis

The paper [5] explores a platform that investigates the decision-making process of Indian users while using Unified Payments Interface (UPI) apps. The researchers created a UPI prototype to engage users in malicious and non-malicious UPI use cases that people experience in real life, but in a virtual, safe environment, that does not gather personal data nor cause a financial attack. Interviews were conducted while the users were using the app and after it, to analyse their thought-process, attentiveness to different scenarios and understanding of the application. The platform utilizes a mixed-method approach, including user surveys, semi-structured interviews, and behavioural data analysis, to uncover the factors that influence users' app adoption and usage. The study finds that perceived usefulness, trust, and security concerns are the critical drivers of UPI app adoption and usage among Indian users. It was observed that there are features like notifications that are known to have major security importance, but was more often than not ignored by the users. Similarly, the amount validation page that includes the sender and receiver's details along with the transaction amount and a message, was commonly accepted in haste.

The paper [6] presents a study that evaluates the privacy and security of mobile payment applications using user reviews. The authors analyse reviews posted on Google Play Store to understand the security and privacy concerns of mobile payment app users. The researchers performed text-based analysis to filter the privacy and security-related reviews and applied sentiment analysis to collect the negative reviews focused on user privacy and security concerns. Furthermore, they performed an in-depth thematic analysis of a subset of these reviews through manual coding and automated analysis. The study identifies the most significant security and privacy concerns, such as transaction failures, data breaches, and unauthorized access to user accounts. One example being - what happens when a user sends money to the wrong person? This is especially important when transactions have been simplified to the extent that just the mobile number of the recipient is enough to complete a transaction.

This analysis helped understand users' perspective of applications that uses UPI and how just making the applications secure doesn't ensure the Security of UPI. Social Engineering is a factor that highly affects users when the applications are easy to setup and use. Any minor information leaked can let an adversary gain access to a user's banks.

III. Evaluating UPI against defined Evaluation Schemes - RBI Guidelines and BASEL Norms

'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: confidentiality, integrity, authenticity and non-repudiation. 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. [3] These guidelines provide an excellent metrics to evaluate the security of UPI based system.

Some of the key findings were such that - 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, apps like Paytm picks up the OTP message, when it is not intended for Paytm. Some of the users expressed concern over this violation of data confidentiality. Grocery delivery apps such as Big Basket can also access Paytm and read the amount available in the bank which is an invasion of privacy. They also deduct money without authentication when an order is placed which poses a security risk.

ANALYSIS OF UNIFIED PAYMENTS INTERFACE USING STRIDE

Based on our understanding of the existing research and our personal experience of using the UPI based PSP applications, we can summarise our findings through a STRIDE Analysis.

- Spoofing: UPI has strong security measures in place to prevent spoofing. The system uses two-factor authentication, which requires a user to enter their UPI PIN and/or biometric information to authenticate a transaction. Once a SIM Card is registered with a UPI Account, a change in SIM will also prevent transactions unless authenticated again. There are loopholes which when exploited, a spoofing attack can be performed but that is subjective to Payment Service Provider Apps.

- Tampering: UPI uses end-to-end encryption to prevent tampering of data during transmission. The system also uses digital signatures to ensure that the transaction has not been altered during transit.

- Repudiation: UPI has mechanisms in place to prevent repudiation. For example, a user must enter their UPI PIN to authorize a transaction, and the transaction is recorded in the user's transaction history.

- Information disclosure: UPI does not disclose any sensitive information to third parties. The system uses tokenization to mask sensitive information, such as the user's bank account number. However, we can see in [3] for a specific case that Paytm allows third party apps to view bank balance.

- Denial of service: UPI is designed to handle a large number of transactions simultaneously, and has measures in place to prevent denial-of-service attacks. For example, the system uses load balancing to distribute the transaction load across multiple servers.

Overall, UPI has strong security measures in place to protect against various types of attacks, and has been widely adopted in India as a convenient and secure way to transfer money.

BEST PRACTICES FOR A SECURE UPI EXPERIENCE

There are several steps that can be taken to prevent UPI (Unified Payments Interface) from attacks and make it more secure:

- Keep your mobile device and UPI app updated with the latest security patches and software updates to address any known security vulnerabilities.

- Use strong passwords and enable two-factor authentication to prevent unauthorized access to your UPI account.

- Do not share your UPI PIN or other personal information

- Always check the transaction details carefully before authorizing a transaction. Verify the recipient's UPI ID or bank account number, the transaction amount, and any other relevant details before proceeding.

- Use only trusted UPI apps that have been downloaded from reputable sources such as Google Play Store or Apple App Store.
- Regularly monitor your UPI account activity and transaction history for any unauthorized transactions.
- Be cautious of phishing attempts that may try to trick you into providing your UPI account details or UPI PIN. Do not click on links or download attachments from unknown or suspicious sources.

  By following these steps, you can help prevent UPI from attacks and make it more secure.

CONCLUSION

In this study we performed an in-depth analysis of Unified Payments Interface through existing research [2][3][4][5][6] and reports. This technology is being used excessively in India and is being adopted by everyone from Students, Corporates to Small Vendors. Having used this technology in India ourselves sparked an interest in us to understand it from security perspective. This study enabled us to see how small errors and details when dealing with a banking system can cause huge security risks. Also, we learnt that Security Evaluation can be complete and comprehensive when performed using different methods like Technical, User and Field Studies, and no one method can completely evaluate the security of a tool as different methods brings forward different results and findings, which are all equally important.

This study discussed the architecture of UPI followed by its capabilities. Furthermore, a security analysis was done on UPI using different methods such as Reverse Engineering, User Interviews, Analysis of User Reviews and Security Analysis based on RBI and Basel Guidelines. This analysis gave up a complete and comprehensive outlook towards the security and usability of the UPI System. The findings were cumulated by a STRIDE Evaluation, and Secure practices for UPI based PSP Apps were discussed.

UPI was launched in India on 11th April 2016 by Dr. Raghuram G Rajan, Governor, RBI at Mumbai. Since then, it has revolutionised how transactions happen in India.

REFERENCES

[1] Unified Payments Interface Product Interview - https://www.npci.org.in/what-we-do/upi/product-overview

[2] Y. Madwanna, M. Khadse and B. R. Chandavarkar, "Security Issues of Unified Payments Interface and Challenges: Case Study," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 2021, pp. 150-154, doi: 10.1109/ICSCCC51823.2021.9478078. https://ieeexplore.ieee.org/document/9478078

[3] Abhipsa Pal, Sai Dattathrani and Dr. Rahul De, “Security in Mobile Payments: A Report on User Issues” - https://www.iimb.ac.in/sites/default/files/inline-files/iimb-csitm-security-issues-in-mobile-payment.pdf

[4] R. Kumar, S. Kishore, H. Lu and A. Prakash, “Security Analysis of Unified Payments Interface and Payment Apps in India”, 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1499-1516 https://www.usenix.org/conference/usenixsecurity20/presentation/kumar

[5] K. Sharma, N. Bajaj, X. Page, M. Mondal, “A Platform for Uncovering Indian Users' Decision-Making Process in United Payment Interface (UPI) Apps” https://www.usenix.org/conference/soups2022/presentation/sharma-poster

[6] U. Kishnani, N. Noah, S. Das, R. Dewri, “Privacy and Security Evaluation of Mobile Payment Applications Through User-Generated Reviews” https://dl.acm.org/doi/abs/10.1145/3559613.3563196