Université libre de Bruxelles

ELEC-H550 - Embedded System Security - 2023/24

Security and Privacy analysis of UPI protocol in PhonePe app

Student Name:

1. Zakaria BELKADI
2. Arun POOVELIKUNNEL VARGHESE

Lecturer in charge:

Prof. Mühlberg Jan Tobias

Submission Date : 26/01/2024

Contents

Abstract

'Unified Payments Interface' (UPI) has witnessed a remarkable surge in popularity in India, in recent times. UPI, operating through electronic devices or online services, serves as a platform facilitating seamless electronic transactions. Essentially, it redefines the payment landscape, offering a paperless method that eliminates the need to carry physical cash and simplifies the entire payment process.
Key players in the Indian UPI scene include popular platforms like Google Pay, PhonePe, Paytm, and others. The objective of this paper is to conduct an in-depth exploration of UPI, and an analysis of potential privacy and security issues given how sensitive personal and financial data is.

1 Introduction

The most commonly used protocol in India by customers to transfer money from one bank to another is RTGS, IMPS and NEFT. These protocols are enabled in the customer's online banking feature, while using this service the sender needs to know the account information of the recipient to transfer the money. The account information includes recipient name, account number, IFSC code of the bank branch in which account holder has the above mentioned account number, phone number etc. So here the many critical pieces of information are shared with a third party [1]. Another factor is the demonetisation of larger currency notes in 2016 also had a large impact on the increased usage of digital banking to transfer money from customers, online and offline merchants [3].

To address the above mentioned problems the Indian government introduced Unified Payment Interface (UPI) as Digital India initiative. The UPI framework was developed by the National Payment Corporation of India (NPCI) which is a consortium of Indian Banks [2]. UPI mode of payment focused on providing a free and instant transfer of money between customers and also without disclosing the critical bank information as well [2]. To achieve this UPI uses a virtual payment address (VPA) called UPI ID or UPI Number.

PhonePe is an Indian digital payment and financial services application founded by Sameer Nigam, Rahul Chari and Burzin Engineer as the name says it is a payment solution for phone users [9]. And went live in 2016, working on Unified Payment Interface, later the product got acquired by Flipkart. They are the largest driver of UPI transactions as a Third Party Application Provider (TPAP) [9]. In PhonePe you can link different bank accounts registered under the same mobile number which make it easier for the user to have access to their bank accounts to send or receive money and even to check the balance. The platform also offers bill payment options integrated with public consumers and private consumers. PhonePe also have micro apps of the third parties by providing many services within the application, so due this various services PhonePe also stores alot of user information and shares with third system needs. PhonePe extends their service to online and offline merchants to accept the money through digital payments, this adds more value to the small scale local merchants to have smooth transactions.[8] [9]

PhonePe is a financial service provider currently following the regulation of the Reserve Bank of India (RBI) and Information Technology Act (IT Act).

In this report we are conducting a privacy analysis of the PhonePe app as it stores potential user information for different functions of the application, our context is more focused on the new digital bill released in August 2023 called Digital Personal Data Protection Bill (DPDP). And we also do the security analysis of the UPI registration process in PhonePe. About the registration process we will discuss further in the report, how it works and what all details and modules are included in the registration process (Fig. 2). [8]

Problem statement

The rapid adoption of the Unified Payments Interface (UPI) has significantly transformed the digital payment landscape in India, leveraging mobile phones as the primary point of access for transactions. As UPI relies on secure mobile payment systems, it is imperative to conduct a comprehensive assessment of potential vulnerabilities within these systems to gauge their impact on the integrity and security of UPI transactions. Moreover, with the impending Digital Personal Data Protection (DPDP) policy in India, it is crucial to examine how it addresses user privacy concerns within the UPI application and compare its provisions with the General Data Protection Regulation (GDPR) in Europe.

2 System Model

This section details two primary processes within the app: the registration procedure and an accompanying information flow diagram. The diagram serves the purpose of identifying the data exchange between users and the UPI server, facilitating the identification of information of potential sensitivity, that will further help conduct a privacy analysis. Simultaneously, a data flow diagram is introduced for security threat modeling, for recognizing and mitigating potential security risks within the app's framework. The DFD will take into consideration transactions that take place after a succesfull registration. Their role is to visually represent the pathways of information within our system of interest, for an easier identification of vulnerabilties.The system will further take advantage of the illicitated mitigations.

2.1 Transactions Data flow diagram

A crucial phase in the data exchange sequence occurs after the registration, specifically when financial transactions come into play. For this phase, a DFD represents the entities and their interaction. This DFD will be particularly handy when threat modeling using the STRIDE framework.

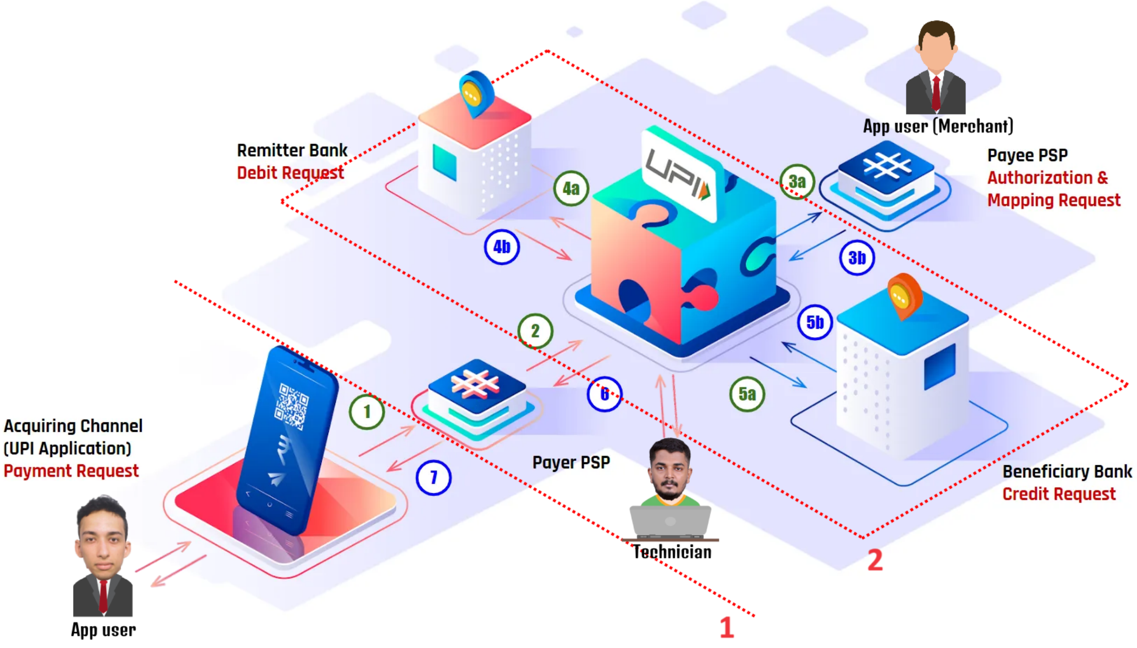


Figure 1: PhonePe DFD [7]

The dashed red line and rectangle illustrated in Figure 1 represent trust boundaries. This seperation is based on the fact that distinct trust levels, were identified between the end device, including the user, and the Payer PSP's server. This seperation is denoted by line 1. Another transition in trust level is between PhonePE's server and the set of servers that process financial transactions, this includes the UPI server, and the banking server which are interconnected. This separated is denoted by rectangle 2.

2.2 Registration Process

The steps 1 to 10 are the various stages of user registration protocol handshake between the Phone Pe and UPI server. The whole registration processes is divided in to two parts: first is device registration or device binding (1-8) which is one time processes per device and the second is the payment registration happen all time when you try to link new bank account (9-10):

1. The user's device information like IMEI number, OS type and version, network type, SIM Number etc. are send to the UPI server as an https request.

2. The UPI server will send a response for the step 1 which includes a registration id, registration token and phone number for step 3.

3. The application will access the SMS module to send the registration token as text message to the phone number. From this step the UPI server will collect the phone number of the user.

4. When the SMS is received the server acknowledge back to the Phone Pe.

5. In this step the same registration token is send to UPI server as https request to validate the device registration is successful.

6. The server will respond if the device binding is successful or not.

7. PhonePe prompts the user to establish a passcode, which consists of four digits

8. the app transmits the effective passcode, generated by hashing the user's passcode concatenated with their phone number, to the UPI server.

9. Once step 8 done, the device binding is complete. the user is required to retrieve their bank information by forwarding the ID of the respective bank.

10. The UPI server responds with the information of the user, in the requested bank.

After completing all the steps mentionned above, the user has successfully linked their desired bank account to the PhonePe app. However, it's important to note that transactions will not be permitted until the user provides the app with the last 6 digits of their credit card, along with the card's expiry date and CVV.

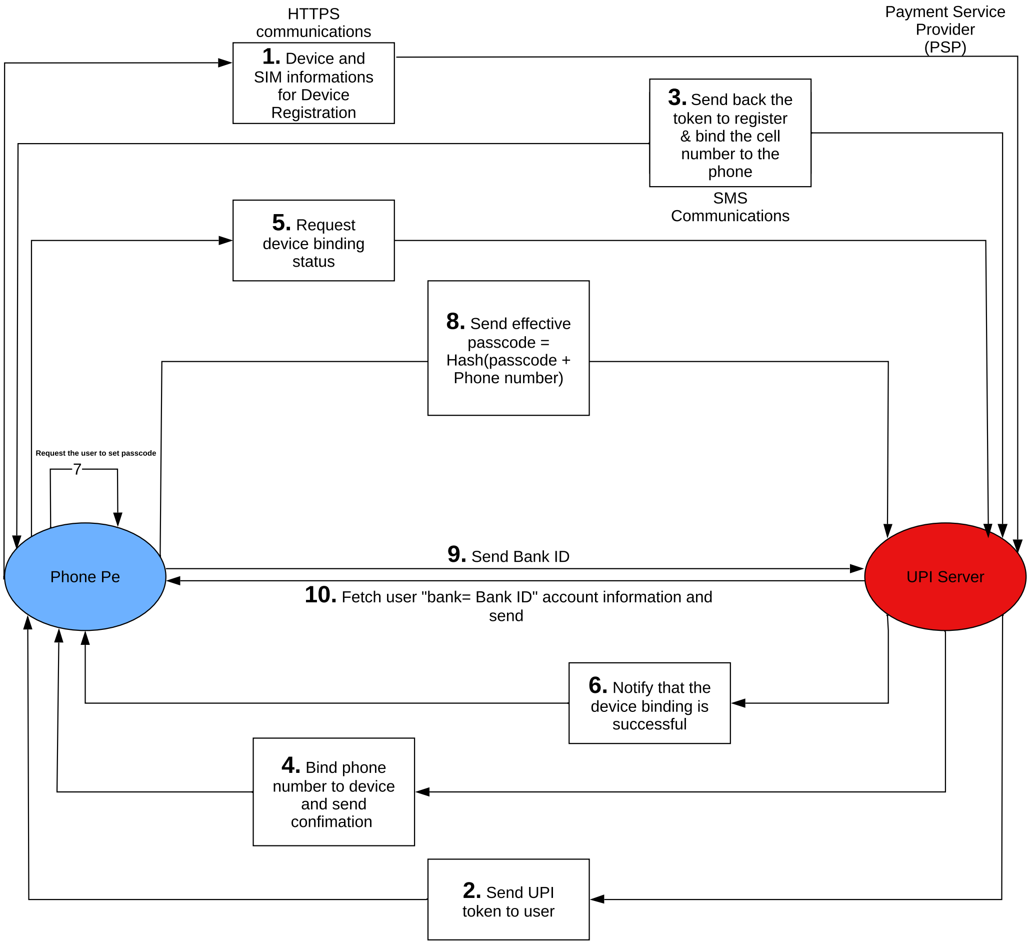

HTTPS communications
1. Device and SIM informations for Device Registration
Payment Service Provider (PSP)
3. Send back the token to register & bind the cell number to the phone
SMS Communications
5. Request device binding status
8. Send effective passcode = Hash(passcode + Phone number)
Request the user to set passcode
7
Phone Pe
9. Send Bank ID
UPI Server
10. Fetch user "bank= Bank ID" account information and send
6. Notify that the device binding is successful
4. Bind phone number to device and send confimation
2. Send UPI token to user

Figure 2: PhonePe Registration process

3 Threat Modeling

Here the threat modelling is done in two perspective:

- The security analysis from a technical perspective focuses on evaluating the robustness of the Unified Payments Interface (UPI) system implemented on phone devices.
- The privacy analysis centers on safeguarding user data within the UPI system, emphasizing the protection of personally identifiable information (PII) and ensuring compliance with privacy regulations.

3.1 Privacy Threat Modeling

Privacy takes a central role, especially in the case of mobile payment applications like PhonePe, where financial transactions unfold, and money is involved. Collecting an adequate amount of data about users, and securing the collection, storage and processing of their personal information becomes therefore paramount. In this section, We will assess the privacy measures in place within UPI systems broadly, more specifically on PhonePE.

3.1.1 DPDP Act Vs GDPR

The Digital Personal Data Protection Bill of 2023 (DPDP) is a legislation in India aimed at addressing privacy and data protection concerns. It seeks to establish a framework to the handling personal data, within the country. Although DPDP draws inspiration from GDPR of the European union, in a sense where it aims to provide individuals with greater control over their personal information by emphasizing consent for example, notable differences highlight GDPR as a more strict and mature legislation, These differences will be highlighted in the following sections.

3.1.2 LINDDUN GO

LINDDUN GO is an accessible variant of the LINDDUN threat modeling framework, presented in the form of a card game. In contrast to the more comprehensive LINDDUN PRO, LINDDUN GO eliminates the need for consulting a mapping table or threat tree catalog thanks to its 35 threat cards. The game is designed to facilitate the identification of potential privacy threats by focusing on LINDDUN threat types:

1. **Linking:** Assessing the potential for establishing connections or links between different pieces of information. LINDDUN GO considers how easily an attacker could link various data points, to help mitigate potential related threats.

2. **Identifying:** Examining the risk of identifying entities within a system, such as individuals or devices. LINDDUN GO helps evaluating how difficult it is to identify entities from their records, whether they are stored, collected or in transition.

3. **Non-repudiation:** Refers in this case to the risk of being unable to deny the validity or origin of a specific action or transaction within a system, which can impact accountability and trust within the system.

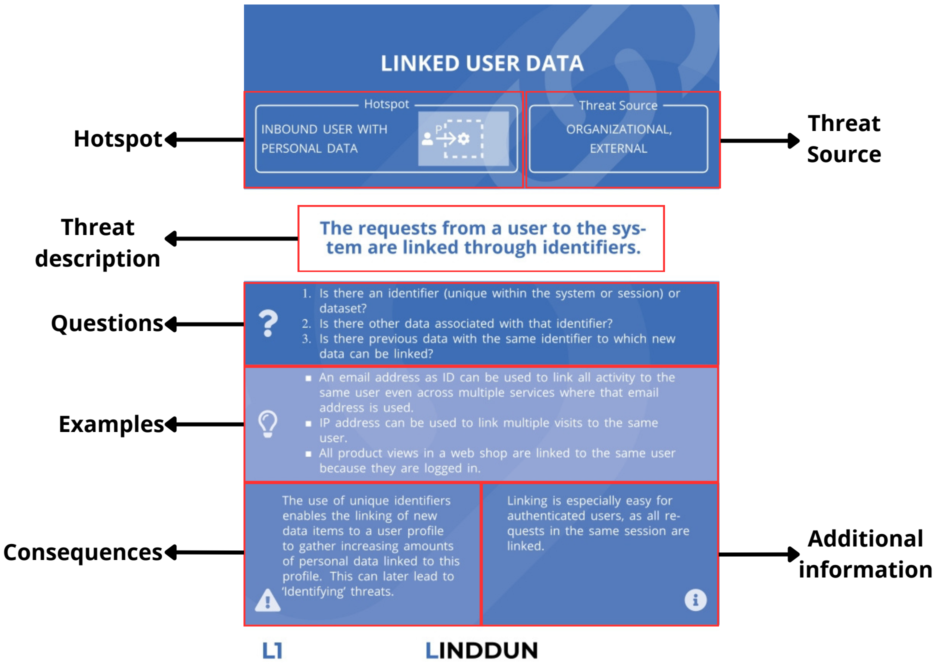
4. **Detecting:** Assessing the ability to deduce or observe the activities or involvement of an individual within a system, which can potentially threaten privacy. LINDDUN GO evaluates the system's design and processes to check whether the deducing of individual involvement is minimized.

5. **Data Disclosure:** Examining the risk of unintentional or intentional disclosure of sensitive information. LINDDUN GO examines if the data minimization principle is applied.

6. **Unawareness:** Refers to when individual lack comprehensive understanding, engagement, or control in the processing of their personal data. LINDDUN GO addresses transparency, valid consent and intervenability.

7. **Non-compliance:** Assessing adherence to security policies, regulations, and compliance requirements.

The cards help adopting a collaborative approach to address privacy issues, making it particularly effective in structured brainstorming sessions involving a diverse team.[10]



LINKED USER DATA

Hotspot: INBOUND USER WITH PERSONAL DATA

Threat Source: ORGANIZATIONAL, EXTERNAL

The requests from a user to the system are linked through identifiers.

1. Is there an identifier (unique within the system or session) or dataset?
2. Is there other data associated with that identifier?
3. Is there previous data with the same identifier to which new data can be linked?

- An email address as ID can be used to link all activity to the same user even across multiple services where that email address is used.
- IP address can be used to link multiple visits to the same user.
- All product views in a web shop are linked to the same user because they are logged in.

The use of unique identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data linked to this profile. This can later lead to 'identifying' threats.

Linking is especially easy for authenticated users, as all requests in the same session are linked.

Figure 3: LINDDUN GO card overview

3.1.3 LINDDUN GO on PhonePE

The fundamental principles of LINDDUN GO being outlined in the previous section, the attention is turned to its practical implementation, within the context of securing data collection, storage and processing, in PhonePe.

1. **Linking**

Threat Name	Description	Assets	Security Measures / Mitigations
Linked User data	Do user requests contain identifiers? If so, can new requests be linked with the existing ones through these identifiers?	Phone Number UPI id Email id	Anonymization, and Pseudo-anonymization are potential solutions (according to GDPR article 29). They do not however solve the problem completely, as they only reduce the linkability. Anonymization is applied in PhonePe according to PhonePe's CTO.
Linking through distinguishable patterns	Given two users data, can they be distinguishable? If so, are the users queried based on these differences?		
Linkable Dataset	Within a database, are users data linked through (quasi)-identifiers?		
Linkable user requests	Does the system work with quasi-identifiers? If so,can they be used to link new data to users?	Card and bank information (last digits of a card don't identify a user by themselves, but if combined with the bank ,they can)	
Profiling Users	Are there patterns in user data, depending on their activities, including timing?	Transaction details (Timing, location, transfer amount)	Profiling users is not addressed anywhere in DPDP act,except for children, which are not PhonePe users. They solution lies therefore in changing the act itself to a more strict one (similar to GDPR).

Table 1: PhonePE Linking Threats

2. **Identifying**

Threat Name	Description	Assets	Security Measure/ Mitigation
Identified User Data	Do incoming requests contain user identity information?	Phone Number UPI ID Email ID	Pseudo-anonymization or anonymization (which is included in DPDP), but it is still a difficult process since linkability could be combined to identify individuals, and it is not addressed in DPDP, which is not the case in GDPR
Identifiable Dataset	Can a given user be identified from database records?		
Identifiable Data	Is data required by the system sufficiently revealing?	Profile Information (PhonePe asks whether a user owns a car, how big is a user's family)	
Identifiable User Requests	Given two users requests or records, are they distinguishable? If so, can users be identified based on these differences?	Device Binding information (Phone Number, UPI ID,...)	
Identifiers in Data Request	When interacting with a User, are (quasi-)identifiers used?	Phone Number UPI ID Email ID Banking information	

Table 2: PhonePE Identifying Threats

3. **Non-Repudiation**

Threat Name	Description	Assets	Security Measure/ Mitigation
Non-repudiation of Service Usage	Can uses deny the usage of a service because of authentication or logs?	Transaction History	In the case of PhonePE, Non repudiation is essential, because of the necessity for compliance with a legal obligation to which the controller is subject. In our case, sending or receiving money is logged for legal reasons (fraudulent transactions).
Non-repudiation of sending	Can users deny having sent a message?	PhonePe and UPI server HTTPS communications (signatures)	
Non-repudiation of Receipt	Can users deny having received a message?		
Non-repudiation of Storage	Can users deny claims about unrepudiable data?	Signed Transactions	
Non-repudiation of Hidden data or Metadata	Do records and requests contain metadata that prevent users from denying claims related to it?	Location	

Table 3: PhonePE Non-Repudiation Threats

4. **Detecting**

Threat Name	Description	Assets	Security Measure/ Mitigation
Detectable Users	Does the system show error messages when retrieving data? Are the error messages different when the item does not exist (versus not having access rights)?	Retrieving account information	Return a generic message for both non existing records and records that a user does not have access to.
Detectable Records			
Detectable Service Usage	Can the communication be observed? Can information be inferred from the observed communications?	Communication between upi server and phonePe	There is no reliable measure to implement here. A proxy or a VPN could be used but its not convenient

Table 4: PhonePE Detecting Threats

5. **Data Disclosure**

Threat Name	Description	Assets	Security Measure/ Mitigation
Excessively Sensitive Data Disclosed	Is the data more sensitive than strictly necessary? Is the data more fine-grained than strictly necessary? Does the data encoding include other (meta)data?	Collecting other information which is not mandatory for payment. And they store and use this information to provide third party services integrated with the app.	DO NOT collect excessive data about the user, which is not necessary for the service to run properly (Data Minimization)

Table 5: PhonePE Data Disclosure Threats

6. **Unawareness**

Threat Name	Description	Assets	Security Measure/ Mitigation
No transparency	Are data subjects insufficiently aware of what personal data is being processed, for what purposes, and in what manner?	Personal data	Enumerated third parties that Phonepe shares the information with, because subjects data, although consented to be shared, are under the policies of the third parties once shared with them.
No privacy controls	Does the system enable the data subject to configure what personal data is processed and for what purposes? Can the data subject alter their preferences afterwards?		Giving the user more access to his data, as indicated in GDPR
No access	Do data subjects lack access to their personal data being collected, processed, stored, or disclosed?		The DPDP bill does not allow the user to alter the data, or to be forgotten. GDPR is an example of regulation that gives a subject more freedom with his data.
No rectification or erasure	Do data subjects have the ability to correct or delete personal data?		Giving the user more access to his data, as indicated in GDPR.The DPDP bill does not allow the user to alter the data, or to be forgotten. GDPR is an example of regulation that gives a subject more freedom with his data.

Table 6: PhonePE Unawareness Threats

7. **Non-compliance**

Threat Name	Description	Assets	Security Measure/ Mitigation
Invalid Concern	Is the consent freely given, informed, specific, and unambiguous? Can consent be withdrawn? Can the consent be demonstrated?	Personal Data	Consent is not freely given (means that you cannot use the service without consenting to the processing of personal data) and the terms and services are also ambiguous. A solution would be to have a consent policy that is clear and less forced on the user.
Unlawful Processing	Does the collection rely on valid, appropriate lawful grounds for a specific purpose? Are there special types of processing such as automated decisions?		AI is used in PhonePe decision making. Transparency is therefore essential.
Automated-decision making			
Disproportionate processing	Does the system collect or process more data than legally necessary?		Family information and other details collected which is not necessary for normal transactions. The mitigation can be data minimization and transparent concern from the user
Insufficient security of processing	Is there a process in place to manage security risks and determine the necessary countermeasures? Does the system have appropriate countermeasures in place to secure the processing of personal data?		Here the proposed mitigation is to do security analysis of the system with a security threat modeling technique like STRIDE

Table 7: PhonePE Non-compliance Threats

Overall, 7 Cards of the LINDDUN GO deck have not been applied, mainly because of the lack of information, that prevent us from answering the questions regarding the threat. The cards are the following:

(a) **Linking:** All cards have been applied

(b) **Identifying:** All cards have been applied

(c) **Non-repudiation:** All cards have been applied

(d) **Detecting:** Detectable events haven't been applied, since we don't know the system's side-effects that are caused by user's actions.

(e) **Data-Disclosure:** Excessively Amount of Data Disclosed, Unnecessary Processing, Unnecessary Storage, Overboard exposure of personal data have not been applied. Overall we don't know how much data is stored exactly, and we don't have a list of third parties that data is shared with.

(f) **Unawareness:** No information when sharing data of others hasn't been applied.

(g) **Non-compliance:** Disproportionate storage has not been applied, since we don't know for how long data is stored within the server's databases.

3.2 Security Threat Modeling

Security is a crucial part of the payment application as we need to address the money and credentials involved in the processing of financial service providers like PhonePe. These are valuable assets of the customer so the system should be designed considering security on top and do security analysis on different cycles to ensure the system is protected against new vulnerabilities. Here we will assess the security measures implied in the PhonePe app using UPI system as primary transaction method. The security analysis is done in the context of UPI application in Phone Pe DFD 1 which involves components taking part in processing the transactions; these are components which have also been part of the registration processes.

3.2.1 STRIDE

STRIDE is a security threat modeling framework to identify and categorize the various potential threats to a system or an application. It is designed in a structured way to analyze the security of the system and the name is an acronym of six different threat categories each one of them focused on different aspects of potential vulnerabilities.[11]

1. **Spoofing (S):** To gain unauthorized access to the system they try to impersonate the user or system. By gathering information from Phishing, vishing and smishing attacks.

2. **Tampering with Data (T):** Tampering threats focus on the unauthorized modification or alteration of data. This can happen during data storage, transmission, or processing, leading to potential integrity breaches.

3. **Repudiation (R):** Repudiation threats are concerned about the deniability of their actions or transactions, creating a lack of accountability.

4. **Information Disclosure (I):** Information disclosure threats involve the unauthorized access or exposure of sensitive information. This can include personally identifiable information (PII) or other confidential data that, if accessed by unauthorized parties, may lead to privacy breaches.

5. **Denial of Service (D):** Denial of service threats aim to disrupt or degrade the availability of a system, rendering it temporarily or permanently unusable for legitimate users.

6. **Elevation of Privilege (E):** Elevation of privilege threats involve unauthorized escalation of user privileges. Attackers may exploit vulnerabilities to gain access to resources or perform actions beyond their intended level of authority.

3.2.2 STRIDE on PhonePe

The practical implementation of STRIDE based on the fundamentals sketched in the previous section, within the context of securing the environment, communication channel, software module and hardware module which help in functioning of PhonePe.

Assets	S	T	R	I	D	E
User Data Banking Data (Bank Details, UPI ID) Personal Data	X	X		X		
Mobile device		X		X		
PhonePe app (code,...)		X		X		X
Physical SIM	X	X		X		
Communication	X	X		X		
Third party integration (merchant, Acquirers, Providers)	X	X		X	X	
Transactions	X	X	X	X		
UPI Server	X		X		X	X

1. **User Information:** User information, including banking data like bank details and UPI IDs, along with personal data such as names and contact details, stands as a crucial asset. This information is important for easy financial transactions and is integral to the core functionality of the system. Protecting this asset is imperative, requiring robust security measures.

   Related Flows: Any data, whether in transit or stored in mobile devices or UPI server.

   Threats: Potential threats to user information as assets include the risk of unauthorized access to user credentials and accounts. This could lead to the compromise of sensitive data, posing a threat to both financial and personal information. Additionally, the lack of due carefulness from users, especially in the face of phishing attacks, represents a significant concern. Users being deceived by malicious entities could result in the disclosure of confidential information.

   Mitigation: Mitigating threats to user information involves implementing Multi-Factor Authentication (MFA) for enhanced access security and encrypting data to protect against unauthorized access. Additionally, while security awareness through communication is a potential measure, its effective implementation is crucial for educating users about potential risks, especially in countering phishing attacks.

2. **Mobile Device:** Mobile Device is the platform or the environment in which the Phone Pe app runs. So from a security point of view the platform also

poses threats which affect the activity application as well as information stored in the application.

Related Flows: Flows between user and mobile device.

Threats: Some of the identified threats are mobile devices with no proper authentication mechanism and outdated operating systems without proper updated security measures.

Mitigation: Having an authentication mechanism by having a strong PIN or biometric verification is to access the applications in the device. Alert the user to do proper OS updates and security patches update provided by the manufacture to have a stable and secure working environment for the Phone Pe app.

3. **PhonePe app (code,...):** The code of an application represents the intellectual property of its developers and the organization behind it. It includes the logic, functionality, and sometimes unique algorithms that provide a competitive advantage.

   Related Flows: Flows between mobile device and PhonePe server.

   Threats: The threat landscape for a UPI application includes the risk of sensitive information exposure if not stored within a Secure storage. Another concern involves the inclusion of cryptographic keys in the code, posing the threat of extraction. Allowing root access to the application increases the risk of unauthorized apps gaining elevated privileges, necessitating the incorporation of root detection mechanisms and code obfuscation. Rooted phones security is also fully dependent on the user, removing any OEM support on the device.

   Mitigation: To enhance the security of the banking app, several measures are in place. Sensitive information, such as credit card details, is securely stored within the Trusted Execution Environment (TEE), employing robust encryption methods to maintain confidentiality. It is the case with Samsung's UPI system, called Samsung pay. Rooted phones, which pose potential risks, are restricted from accessing the app to prevent security vulnerabilities like unauthorized access or alterations to the app's code. The app should employ a signing mechanism for its binaries, ensuring the integrity of the code and mitigating the risk of tampering. Secure key management practices, including regular rotation and secure storage, contribute to overall resilience against potential cryptography threats.

4. **Physical SIM:** The physical SIM card is one of the key hardware components for the functioning of Phone Pe app. The physical SIM is mandatory to bind the device. The Phone Pe can access the information about the SIM in the various stages of the device registration.

   Related Flows: Flows between user and mobile device (Physical theft), and between mobile device and PhonePe server (Registration and authentication).

   Threats: The threat related to SIM and it's activity arise the risks, SIM swapping by manipulating the SIM card provider to issue new SIM card, SIM cloning by obtaining unique identifiable information and cryptographic key store in SIM to make a replica, malware running on mobile device can steal SIM information, physical theft of SIM card and insider threat in SIM providers side.

Mitigation: Enable a PIN protection option for SIM and change the default PIN to a new one. Also enable the feature to encrypt the SIM information. Create an awareness between user and SIM provider employee regarding the threats. Monitor SIM card activities includes checking the usage and billing information.

5. **Communication:** Communication regroups all types of interactions among the user, the payment PSP server, and the UPI server, at binding or transaction stages. This interaction involves the transmission of sensitive data, including financial credentials and phone numbers. It is imperative to ensure the security of this communication, safeguarding it against any unauthorized alteration or leakage.

   Related Flows: All flows between a mobile device and UPI server.

   Threat: Unauthorized access to communicated data poses a serious risk in the context of digital payments. It involves the potential breach of the UPI system, allowing unauthorized entities or malicious actors to gain access to sensitive information exchanged during transactions. This could lead to unauthorized access to user accounts, compromising personal and financial details.

   Mitigation: Robust encryption protocols and multi-factor authentication, are crucial to mitigate this threat. The UPI protocol implies the use of HTTPS communications, which already include encryption, integrity and authentication.

6. **Third party integration (merchant, Acquirers, Providers):** The application also provides support for various services for online and offline merchants which enable the third party application to make use of the UPI enabled transaction with the Phone Pe. Phone Pe has three different acquisitions in the case of UPI protocol for providing the VPA to users and there are other third party application services that make use of information stored in Phone Pe to provide better business solutions.

   Related Flows: Flow between the payer and the payee using UPI applications.

   Threats: Phishing to collect the information about the user, calls or emails or text messages from the pretending acquirers. Replacing the QR code of merchants to collect information or changing the payee details to manipulate the transactions. Distributed Denial of Service attack of cloud services of the third parties by making the user to not access or perform the services.

   Mitigation: Create awareness about such calls or emails and text messages which are intended to collect your personal information. While scanning QR codes check if it is a valid UPI ID, if not alert the user to stop the transaction. And also have a feature to limit the transaction amount. Upgrade the cloud system with an anti-DDoS system to have safe and secure business transactions.

7. **Transactions:** Transactions and communication share are similar and subject to similar threats. Transactions, represent a specific subset of communication, including the exchange of financial details between a sender and a recipient. Both processes involve the transfer of information, and the risks associated with securing this information are inherent in both transactions and communication. In the context of transactions, the focus is on the secure exchange of financial data.

   Related Flows: All flows between a mobile device and UPI server. Similar to communications.

   Threats: The potential threats to transactions involve the unauthorized access or alteration of transaction data,which is a risk of tampering with or gaining unauthorized entry to the information exchanged between parties. This can lead to money getting sent to wrong recipient, or money getting sent in the wrong amount. Additionally, there is a concern for fraudulent transactions, where malicious actors manipulate or exploit the transaction process for their own benefits.

   Mitigation: To enhance transaction security, robust measures are deployed. Transaction data is encrypted, safeguarding sensitive financial details from unauthorized access or alterations. Access control mechanisms limit and manage access to transaction information, reducing the risk of internal or external unauthorized entry. Continuous monitoring, using AI, detects transactions, enabling timely intervention to prevent fraudulent ones.

8. **UPI Server:** The UPI server is the core of the Unified Payments Interface, enabling transactions between users and banks. It supporting interoperability across different banking institutions.

   Related Flows: Flows between mobile devices and UPI server, but also between technicians and the UPI server (Unauthorized access).

   Threats: The UPI server faces threats such as unauthorized access, unauthorized actions, and denial of service. Unauthorized access could compromise sensitive information, while unauthorized actions may lead to fraudulent activities. The risk of a denial-of-service attack poses a concern for disrupting the server's availability.

   Mitigation: To mitigate UPI server threats, Two-Factor Authentication (2FA) is implemented for enhanced access security. Regular server audits and monitoring quickly address anomalies, ensuring transaction integrity. Denial of Service (DoS) protection measures defend against disruptions from malicious attacks, ensuring consistent service availability. Enforcing the principle of least privilege restricts server access, minimizing the impact of potential security breaches.

3.2.3 Ranking the Security Mitigation

We have seen different mitigation methods for the set of assets and these mitigation has been prioritized based on the affected area and impact of the threat on the system.

1. High: These categories of mitigation mainly focused on the smooth functioning of the application. So the mitigation will be on the PhonePe app or

the connected system. Some of the mitigation are MFA, encryption of data in transit,QR code verification & notification when QR code is not a valid UPI ID, Usage of TEE to store encrypted sensitive data, Signing binaries, Secure key management, Enforce minimum privilege, Regularly audit and monitor the server and implement DoS protection. Regarding the encryption in data sharing the PhonePe uses https communication and as MFA it uses One-Time-Pad (OTP) only at the stage of registration and creation of UPI PIN, afterwards on daily transactions it just uses the UPI PIN and there is no more MFA.

2. Medium: This category of mitigation has an impact on the environment in which the application is running and auditing system. Some of those mitigation are Ban rooted phones from using the app, Raise awareness of users and SIM provider employees, Security awareness by communication (not implemented) and Monitor and detect abnormal transactions.

3. Low: Some of these measures are already existing and advise users to make use of those measures which will provide an add-on security layer for the application and activity involved in the app. The mitigation includes Enable PIN protection, SIM card data encryption, Monitor your SIM card activity (usage and billing information), Update the OS whenever a new version is available and Limit transactions amount.

4 Conclusion

In this report, we explored the UPI system, with a closer look at PhonePe. We analyzed privacy threats using Linddun Go, based on GDPR, revealing variations in privacy approaches between India and the DPDP Act, as shown in the table 8.

Aspect	**General Data Protection Regulation (GDPR)**	**Digital Personal Data Protection Act, 2023 (DPDP Act)**
Scope	Applies to all organizations processing personal data of individuals in the European Union, regardless of the organization's location.	Applies to all organizations processing personal data of individuals in India, regardless of the organization's location.
Consent & subject rights	Requires explicit consent from individuals before processing personal data. Subjects have the right to be forgotten, and profiling users is restricted.	Allows processing of personal data without consent in certain cases, such as performance of a contract or in the public interest. Subjects do not have the right to be forgotten and profilling users is possible, except for children.
Data Localization	Requires organizations to store personal data of individuals in the European Union unless certain exemptions apply.	Does not mandate organizations to store personal data in India.
Data Breaches	Requires organizations to notify the relevant data protection authority within 72 hours of becoming aware of a data breach.	Requires organizations to notify the Data Protection Board and affected individuals within 72 hours of becoming aware of a data breach.
Penalties	Imposes fines of up to €20 million or 4% of global annual turnover, whichever is higher.	Imposes fines of up to INR 250 crores.

Table 8: Comparaison of GDPR and DPDP

Our attention turned subsequently towards security threat modeling, employing the STRIDE framework. This involved an enumeration of assets, identification of potential threats, and the proposal of corresponding mitigations. Notably, a substantial proportion of the suggested mitigations has already been put into effect.

5 References

[1] Towards Formal Modeling and Analysis of UPI Protocols https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9388452.

[2] Security Analysis of Unified Payments Interface and Payment Apps in India https://www.usenix.org/system/files/sec20summer_kumar_prepub.pdf.

[3] Cyber-Security in UPI Payments https://www.ijraset.com/best-journal/cybersecurity-in-upi-payments.

[4] Security in Unified Payments Interface and Payment Apps in India http://www.ijirset.com/upload/2020/july/46_Mr.Sachin%20Shende_DT.PDF.

[5] A Study of Threat Model on Mobile Wallet Based Payment System https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3361202

[6] Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures https://www.researchgate.net/publication/332113623_Wallet_Payments_Recent_Potential_Threats_and_Vulnerabilities_with_its_possible_security_Measures

[7] How Do UPI payment works? https://medium.com/dice-india/the-enabling-power-of-upi-payments-4060826c2a16

[8] PhonePe https://www.phonepe.com/about-us/

[9] PhonePe Wiki https://en.wikipedia.org/wiki/PhonePe

[10] LINDDUN GO https://linddun.org/go/

[11] The STRIDE Threat Model https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN