

Secure Systems and Applications

COMM047: Coursework 2

**Security and Privacy
Overviews In Mobile Payments**

I declare that this report is my own work

Aran Jansson

January 13, 2026

1 Abstract & Introduction

Abstract

Mobile payments are used in day to day life, from paying for online bills to paying for food in your local shop. These payments are usually one of two forms: SMS-based mobile payments and mobile wallet based payments. Whilst both offer their own benefits, they both come packaged with their own security and privacy trade-offs. SMS payments provide a wider range of coverage allowing for service in less technologically developed regions, digital wallets can provide a faster and more secure form of mobile payment in a more limited geo coverage. These systems rely on secondary technologies such as GSM networks, Near Field Communication as well as One Time Passcodes in order to provide their services. In this essay, the security and privacy of these technologies are explored and compared to provide a better understanding of the benefits and drawbacks of each system, as well as providing information on currently available alternatives and new possible areas in which mobile payments can grow to better serve the goals of privacy and security.

Introduction

Mobile payment methods designed in recent years take advantage of a full connectivity approach in order to complete a transaction, having all devices used during a payment being connected to some form of banking service. This provides instant confirmation in order to verify a payment and complete the transaction in a matter of seconds. This methodology works functionally well in developed regions; however, it is flawed in areas with low network coverage and completely voids the ability to conduct a payment anonymously as the payee's bank is directly contacted for each transaction that takes place.

Processing user information for a payment between multiple devices and servers can be seen as a breach of privacy as the data regarding the payment runs the risk of being intercepted and or incorrectly secured from one node to the other. In addition, user anonymity is non-existent in systems such as these as the user's identification details are used between each stage of the communication leading to the possibility that a user's data could be stolen and or misused. Services that rely on Global System for Mobile Communications (GSM) networks also run the additional risk of the communication being intercepted and altered due to the insecure cryptographic schemes in use. Some researchers have attempted to develop ways to provide increased anonymity in the world of mobile payments, taking advantage of technologies such as blockchains and One Time Passwords, completely diverging from the use of direct token based mobile payments as well as GSM based transactions.

2 Literature Review

2.1 Global System for Mobile Communications

GSM Networks provide the modern day standard for direct communication between multiple parties. First being introduced as a second generation (2G) digital communication protocol in 1991, it provided a way to send encrypted traffic between users with a higher level of security. GSM supports features such as SMS and MMS, allowing non verbal communication through text and images to be possible [20].

2.2 SMS-Based Mobile Payments

SMS-Based Mobile payments were designed in order to enable users to complete and verify payments using the GSM network. A retailer would send the user an SMS message including details on how to complete a payment. This could be a number in which the user can send an SMS with the amount to be paid to the merchant. The benefits of SMS-based payments is that GSM networks have a wider coverage than 3G/LTE/5G networks, allowing for payments to be made in a wider range of locations making it a primary technology for financial services serving regions with underdeveloped infrastructure. Although these services provide a wide range coverage that no other mobile payment technology is able to provide, SMS-based payments come with their own disadvantages in the form of security and privacy with the technology relying on outdated A5/1 or A5/2 stream ciphers to transmit SMS messages [3, 5].

2.3 One Time Password (OTP)

One time password provides an additional form of verification based on a secure single use framework. When a payment request is received, a code in the form of integers or strings is generated, and is forwarded to the user. This code in nature is generated securely by accessing information, such as the current timestamp, to provide randomness to the code. The time stamp would then get hashed or encrypted using a private and public key pair, in which the keys are generated locally, and the public key is provided to the server in order for it to encrypt the code and forward it back to the user. If the user is able to decrypt this value and gain the original one time password, the payment would be authorised, hence proving their identity. The encrypted code would have been delivered to the user using their email address or mobile phone number registered to their bank or financial institution [13, 6, 8].

2.4 Mobile Payments Using Near Field Communication (NFC)

Near Field Communication (NFC) is a technology which allows the transfer of information wirelessly between two points within a limited range. Small packages of data such as a phone number, coordinates, and even payment information can be passed between two NFC enabled devices when pairing is established. NFC can be taken advantage of in order to enable wireless mobile payments that do not rely on SMS technologies, completely bypassing the need for OTP to verify payments. To validate NFC payments, the user would have a device, which is protected by either a passcode or biometric authentication system. When a user attempts to conduct a payment using this system, the payment device would first check if the payment is authenticated by the device administrator by checking if they have unlocked the device, and how long it was unlocked. If the device is unlocked and a substantial amount of time has not passed, the device automatically approves any contactless payment made via NFC using the user's credentials to sign and confirm the transaction.

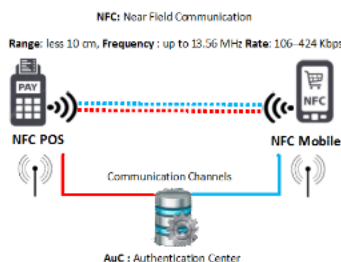


Figure 1: NFC Payment Example [1]

The data transferred between the two NFC points would be information such as a one time card number generated by the payee device in order to provide security preventing theft of card details. The merchant side would then process the payment based on this card information, and an authentication centre of the card issuer will approve the payment by contacting the original card issuer's bank to complete the purchase. [16, 9].

2.5 Mobile Payment Wallets

Mobile payment wallets provide a centralised hub in which a user can store any supported payments cards, allowing them to use any of these to complete a contactless mobile transaction using their smartphone or smart watch. When a user wants to add a credit or debit card to the wallet, the wallet checks the details with the card issuer and generates a token that is stored locally on the device. These wallets take advantage of NFC technology in order to transmit this token, which acts as a mask, to the original card number, ensuring that the original card number is not directly shared with the merchant.

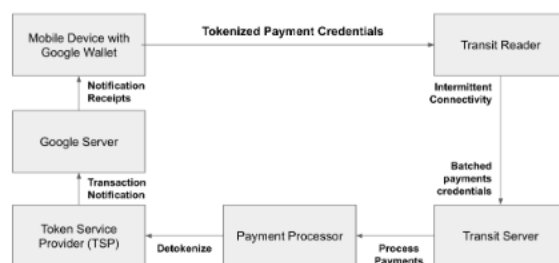


Figure 2: Google Pay Transaction Scheme [18]

For every transaction, the wallet generates a unique signature to confirm authenticity. Even if a malicious user intercepts the NFC payment signal, due to this signature they would not be able to steal payment card information or money because of the signature being of limited use such as a one time signature, allowing for increased security in mobile payments using these types of wallets compared to other contactless payment schemes [15].

2.6 Passkeys For Authentication

Mobile payments schemes can also take advantage of technologies such as passkeys in order to verify the user. This could be a system such as a two factor authentication where the implementation of a passkey, which is a unique key specific to the current device that cannot be altered or changed after being generated in order to be used for verifying the user's authenticity [14]. Passkeys could be applied to mobile payments by the user using biometric authentication methods such as a built in fingerprint scanners to verify a challenge sent from a server which stores the public key related to the passkey being used, whilst the fingerprint would then unlock the passkey in order for it to be used to decrypt the challenge. This can be used to verify a purchase instantaneously. The benefits of a passkey are not just limited to security, but they also provide privacy benefits as a user can be cryptographically verified without giving the service any additional information.

Passkeys complement security as well as privacy as the merchant would only be provided with an approval status for the payment if the challenge was completed successfully. When a payment is approved, the payment service can communicate with the bank to request the sum spent without the merchant knowing which account the money is being taken from directly.

3 Security and Privacy of Mobile Payments

Security of mobile payments schemes vary based on which technology is in use. Each system aims to solve a unique problem, whilst others try to replace an outdated protocol. This can be present with the jump from SMS based payments to mobile wallets where mobile wallets have largely faded out SMS based payment protocols. The main drive for this is usability as well as the overall security of these protocols.

3.1 SMS-Based Protocols

SMS Based protocols generally apply the A5/1 and A5/2 protocols, which take advantage of pre existing GSM networks. The encryption of these protocols provided use outdated symmetric key stream ciphers in order to encrypted and transmit SMS data. A5/1 uses a set of three stream cipher registers of size 19, 22 and 23 bits respectively. Each register has its own clock value in order to allow for non linearity and deciding the final output value based on the greater of these three registers. Whilst A5/2 includes the same number and sized registers, it also includes a fourth register of 17 bits. This fourth register is in charge of deciding which one of the three original stream cipher will be used as the final output [3, 5].

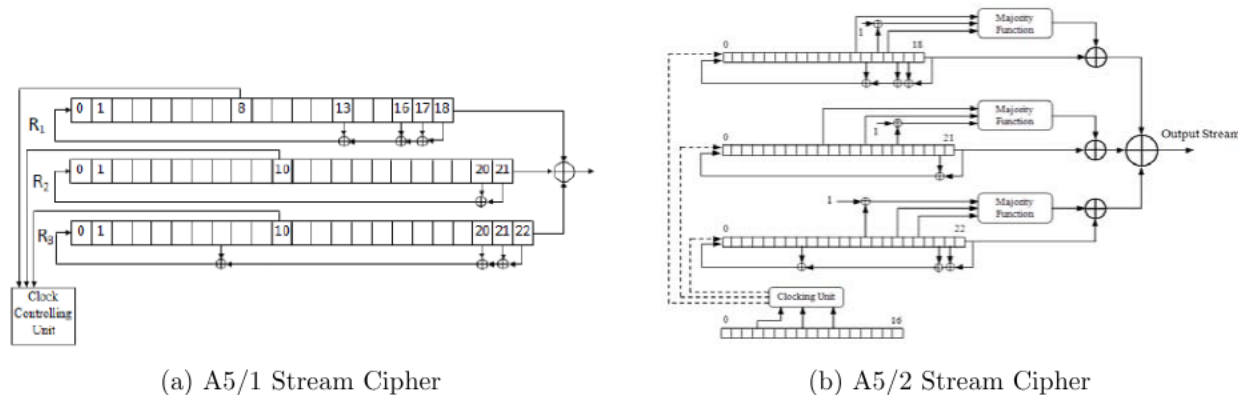


Figure 3: A5/1 and A5/2 stream cipher algorithms [3]

Security

The main downside of these in regards to privacy as well as security is due to the size of keys being used as well as the general scheme itself. A5/1 uses 64 bit symmetric keys to provide an LFSR encryption, whilst A5/2 is even weaker than this using 40 bits as the total key length. These systems are cryptographically weak by modern standards, with modern computers being able to decrypt messages sent on these platforms quickly. When the schemes were originally introduced, the platforms were able to provide the necessary security required at the time. However, this did not last for very long as the encryption technology these are based on was deprecated by NIST [12] in 2005. The weak nature of these two protocols provide a major security risk for people sending

valuable data through SMS channels on the GSM framework. This in particular is a major risk to SMS-based mobile payments as if a message gets intercepted, a person attempting to make a payment may end up with the payment going to the wrong location due to someone decrypting his message, possibly redirecting or even altering the message. [5]

Privacy

Systems using these protocols contain major privacy risks as previously stated due to the insecure nature of A5/1 and A5/2 where a user's message can be intercepted and read without the senders knowledge. This is due to the linearity and predictability of LSFR streams. Malicious users can gain access to financial information stored in the SMS such as card numbers and OTP codes. In addition, as SMS payments use GSM networks in order to function, an attacker can gather information about the user's current location.

3.2 Wallet Based Payment Protocols

Mobile payment wallets provide a service in which users can use their mobile devices to complete payments using contactless NFC technology. The security of such schemes are shown to be drastically higher than of A5/1 and A5/2 based GSM SMS payment methods. Mobile payment wallets take advantage of tokenization to provide a more secure and private payment method.

Security

NFC based mobile payment systems require high levels of authentication as well as trusted systems to be in place. These systems use pre-existing payment standards used in standard card based contactless payments such as EMV [17]. EMV introduces the requirement of chip based authentication in order to validate purchases by requiring the user to include a pin code alongside the payment card. In mobile wallet based NFC payments, EMV technology is still in use providing authentication and a pin based on data stored on the device's profile for the specified card. When a purchase is made, a unique token generated by the mobile wallet is used in order to authorise and complete a transaction. Each purchase is verified using biometric technologies or pass codes on the user's device, preventing any transaction from taking place until this authentication step is completed. In addition, contactless NFC technologies in use are applied to only function from a short distance, preventing a payment from taking place if the mobile device is not close enough [17], reducing the likelihood that an attacker can eavesdrop on the communication.

Privacy

The privacy of mobile wallets carry a vast number of questions. Due to the nature of the system and the fact that the device, bank as well as the wallet of choice will have to store information about any card linked to the wallet and transactions that take place. Many questions can be raised regarding privacy: the use of a digital wallet allows for increased privacy for external third party users such as the merchants that the digital card is used at, the users information still has to be verified in one form or another. The merchant's bank and the receiver's bank do a final communication in order to complete the transfer of funds [2, 17].

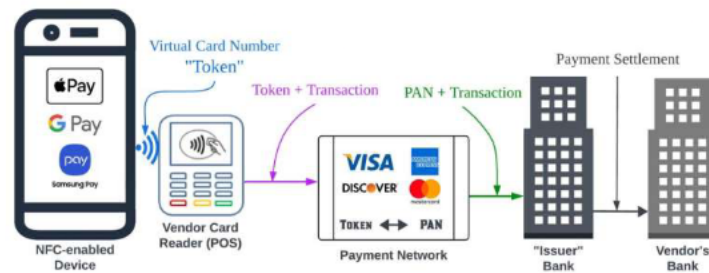


Figure 4: Mobile Wallet Payment Communication Diagram [2]

When a payment is made using NFC to a card reader, the card's token value is transmitted to the card reader. This information is then processed by the the payment network in conjunction with the bank linked to the token. The bank then communicates with the merchant's bank in order to complete the transaction.

4 Security & Privacy Trade Offs

In mobile payments privacy trade-offs are often made in order to provide a more reliable and secure platform. Systems such as mobile wallets are an example of this. The system provides a high degree of security for the end user by implementing tokenisation to provide a virtual card number to a merchant rather than the raw card number itself. However, in order to provide this, multiple checks must be applied during each purchase, which voids a level of privacy to allow for the prevention of fraud. The line that is drawn between privacy and security is extremely fine for mobile banking as they can view what transactions a user is making in order to provide more personalised recommendation, as well as services such as a categorised budget calculator [4]. The trade offs may be seen as reasonable by the average consumer. However, people who have a deeper understanding of how these technologies work may not be as willing to provide multiple institutes with their personal information. Whilst the merchant is able to save a record of basic user information for a transaction [15] such as their name, a bank that is involved in this communication could theoretically be able to see how much a user has spent and at what store without the user being directly aware.

Nonetheless, some of these privacy trade-offs provide benefits for the end user as they provide protection against financial fraud. The requirements of biometric authentication can be one example of this. If a user attempts a payment, the only way in which this payment will succeed is if the user verifies their identity using their fingerprint or face scan. Although this data is not directly shared outside of the user's device, a passkey is kept on record on servers, allowing payment providers to know that it is still the same person making the current purchase. Since this passkey will be saved alongside the users credentials such as their name and address, it would be easy for the two detail sets to be put together in order to confirm that the purchase signed off by the valid passkey is owned by the person on record. This lapse in privacy for the user however comes with the previously mentioned security benefits as the user is verified in multiple ways before a purchase can be made. These are but are not limited to the user having to first be logged in, verify their identity using biometrics before tapping their NFC device on the payment terminal [15, 9], or even being provided with an OTP [6] to complete a purchase.

The flip side of the coin would be security limitations in order to provide anonymity and privacy for a user. A payment can still be accomplished by a user without as much data being necessary by disabling biometric authorisation for a purchase, allowing the purchase to technically have been made by anyone with access to the device. This can allow the user to have a basis for deniability of a purchase in which they can state a close family member such as a spouse to also have access to the device and its payment methods. On face value, when a purchase is made, the card owners details will however still be present, allowing for banks to provide the argument that any purchases made with this card is done by the owner and or by their explicit permission, still linking the owner to any purchase even if not as directly.

5 Existing Solutions & New Ideas

5.1 Anonymity Based On A Client Centric Model

Current mobile payment services such as Visa's 3D Secure [7] protocol provide the assumption that all devices involved in a transaction are connected to internet. This provides restrictions for mobile payments if a transaction is attempted outside of a coverage zone. In order to counteract this, a proposal was made for a client centric model [10] to provide a secure anonymous payment system even if there is no network connection to the payment terminal. The way this system would function is by having the merchant send an encrypted transaction to the payment device, such as a mobile phone using contactless payment, which includes the information regarding the transaction. This can be done by using technologies such as Bluetooth or Near Field Connectivity (NFC). The payment device would then connect to the payment service, such as a bank, processing all the information for the payment locally [10].

5.2 Anonymity Using Blockchain Technologies

Blockchain technologies provide new possibilities for both security and anonymity. Blockchain technologies work by storing data in blocks across multiple systems in the form of a linked chain. This provides a feature set in which each entity in the chain is linked to one another based on the time the data was added to this chain. When a new block is added, it mathematically links itself to the previous block to maintain data integrity [19]. Blockchain technologies can be taken advantage of to provide anonymity due to its mathematical nature of linking to the previous block. A chain can be generated on a user's payment device, provide proof of ownership of funds or an account. Instead of storing a complete history of all transactions, the payment system maintains and can generate two separate blockchains, one that stores partial transactional data and one that stores account data. A third chain can be created in order to store all transactional information in order for it to be used as proof of ownership of an account or balance. Only necessary data related to the transaction is stored [11]. In order to provide anonymity, the system would use threshold based Schnorr Signatures [11]. This system allows a group of users to create a set of keys in which all transactions attempt by any individual in this group appears to come from the group rather than an individual [11]. If someone was to have a look at a transaction made using this system, they can see that someone in the group signed the transaction, but they cannot tell who specifically signed it, allowing sender anonymity [11]. When the signature is verified, an update is initiated on the transaction chain in order to validate the usage of the funds from the user's account.

5.3 Possible New Idea

A possible new implementation could be a system that relies on passkeys and blockchain technologies [19] to locally compute a transaction. In order to balance privacy and security to a better degree, a system could take advantage of self stored dynamic passkeys. This would function in a fashion in which the passkey is regenerated after a set amount of time is passed and is then sent as an encrypted communication to the bank associated with the account in use. When the bank receives the new passkey, it automatically overwrites the one currently stored. These passkeys can be linked together in a blockchain to verify an old passkey if needed by the users on their local machine. The bank would only receive limited information on purchases made, such as possibly only linking the amount spent by the user, whilst the balance transfer's final destination would only be computed by the mobile device being used for the purchase. If a system such as this one could be made, it would allow for a better balance between secure payments whilst also preserving a higher level of privacy and anonymity.

6 Conclusion

Overall, mobile payment systems provide varying levels of privacy and security based on the technology used. SMS-based protocols provide the least amount of security and privacy, whilst wallet based payment systems are more secure. However, they require a higher level of personal information in order to function. Solutions that rely on client centric approaches as well as those which take advantage of blockchain in order to mask the user's identity provide effective implementations to be used. With the possibility of further new ideas, the privacy and security trade off in the current mobile payment market could improve based on the willingness and compliance from global banking leaders.

References

- [1] https://www.researchgate.net/figure/NFC-mobile-payment-application-parties_fig1_324954191.
- [2] <https://techxplore.com/news/2024-08-reveals-loophole-digital-wallet-rightful.html>.
- [3] Majid Bakhtiari and Mohd Aizaini Maarof. "An Efficient Stream Cipher Algorithm for Data Encryption". In: *International Journal of Computer Science Issues* 8.3 (2011), pp. 247–253. ISSN: 1694-0814. URL: <https://www.ijcsi.org/papers/IJCSI-8-3-1-247-253.pdf>.
- [4] *Budget Calculator* — lloydsbank.com. <https://www.lloydsbank.com/help-guidance/support-and-wellbeing/managing-your-money/budget-calculator.html>.
- [5] Imran Erguler and Emin Anarim. "A modified stream generator for the GSM encryption algorithms A5/1 and A5/2". In: *2005 13th European Signal Processing Conference*. 2005, pp. 1–4.
- [6] Silke Holtmanns and Ian Oliver. "SMS and one-time-password interception in LTE networks". In: *2017 IEEE International Conference on Communications (ICC)*. 2017, pp. 1–6. DOI: 10.1109/ICC.2017.7997246.
- [7] *How does 3D Secure authentication work?* — Stripe — stripe.com. <https://stripe.com/en-nl/resources/more/3d-secure-101>.

- [8] Wen-Bin Hsieh and Jenq-Shiou Leu. “Design of a time and location based One-Time Password authentication scheme”. In: *2011 7th International Wireless Communications and Mobile Computing Conference*. 2011, pp. 201–206. DOI: 10.1109/IWCMC.2011.5982418.
- [9] Emir Husni et al. “Efficient tag-to-tag near field communication (NFC) protocol for secure mobile payment”. In: *2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering*. 2011, pp. 97–101. DOI: 10.1109/ICICI-BME.2011.6108602.
- [10] Jesus Tellez Isaac and Jose Sierra Camara. “Anonymous Payment in a Client Centric Model for Digital Ecosystems”. In: *2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference*. 2007, pp. 422–427. DOI: 10.1109/DEST.2007.372011.
- [11] Jianeng Miao and Zhen Han. “An Decentralized Anonymous Payment Confidential Transactions with Efficient Proofs and Scalability”. In: *2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)*. 2022, pp. 1347–1351. DOI: 10.1109/EEBDA53927.2022.9744784.
- [12] *NIST Withdraws Outdated Data Encryption Standard* — *nist.gov*. <https://www.nist.gov/news-events/news/2005/06/nist-withdraws-outdated-data-encryption-standard>.
- [13] Eddy Prasetyo Nugroho, Rizky Rachman Judhie Putra, and Iman Muhamad Ramadhan. “SMS authentication code generated by Advance Encryption Standard (AES) 256 bits modification algorithm and One time Password (OTP) to activate new applicant account”. In: *2016 2nd International Conference on Science in Information Technology (ICSITech)*. 2016, pp. 175–180. DOI: 10.1109/ICSITech.2016.7852629.
- [14] *Passkey: Simple and Secure Passwordless Sign-In - Safety Center* — *safety.google*. <https://safety.google/safety/authentication/passkey/>.
- [15] Tooba Qasim, Sidra Siddiqui, and Shafiq ur Rehman. “Interactive shopping with mobile wallet”. In: *World Congress on Sustainable Technologies (WCST-2012)*. 2012, pp. 32–36.
- [16] Aye Mi San and Chanboon Sathitwiriawong. “Privacy-preserving offline mobile payment protocol based on NFC”. In: *2016 International Computer Science and Engineering Conference (ICSEC)*. 2016, pp. 1–5. DOI: 10.1109/ICSEC.2016.7859939.
- [17] Rainer Schamberger, Gerald Madlmayr, and Thomas Grechenig. “Components for an interoperable NFC mobile payment ecosystem”. In: *2013 5th International Workshop on Near Field Communication (NFC)*. 2013, pp. 1–5. DOI: 10.1109/NFC.2013.6482440.
- [18] *Technical architecture — Open loop transit — Google for Developers* — *developers.google.com*. <https://developers.google.com/wallet/tickets/open-loop/setup/technical-architecture>.
- [19] *What Is Blockchain?* — *IBM* — *ibm.com*. <https://www.ibm.com/think/topics/blockchain>.
- [20] *What is GSM? Global System for Mobile Meaning* — *Wireless Logic* — *wirelesslogic.com*. <https://wirelesslogic.com/iot-glossary/what-is-gsm>.