A Comprehensive Study of Google Wallet as an NFC Application

Omkar Ghag
Thadomal Shahani Engineering College,
India

Saket Hegde
Thadomal Shahani Engineering College,
India

ABSTRACT
The advent of Near Field Communication (NFC) has given rise to several interesting applications under short-range radio technology. Perhaps the most exciting of these is card emulation. Launched in September 2011 [23], the "Google Wallet" application is one of the frontrunners of this technology. More than a year after its launch, there is clearly much interest in the commercial potential of mobile wallets by a variety of organizations in the communications and financial industries and beyond. This paper describes the working of NFC and contactless smartcards along with a brief introduction to the said mobile payment system. It also provides an evaluative study on the operation and performance of Google Wallet. A comparative study of Mobile Payment Solutions is also elucidated. Past and existing vulnerabilities of the system are discussed in detail along with noteworthy examples of infiltrations. The significant threat vectors to an NFC enabled mobile device are also examined with practical attack scenarios. Additionally, safeguards that the Wallet currently uses are evaluated. The paper is concluded by pondering on if and when such systems will become as ubiquitous as the physical wallet. For the reader's reference, the phrase "Google Wallet" in this paper refers to Google Wallet version R79v5 as of September 2012

General Terms
Mobile Payment, Virtual Wallet, Near Field Communication.

Keywords
Google Wallet, Near Field Communication, Smart Card, Attacks, Security.

1. INTRODUCTION
Near Field Communication (NFC) is an upgraded version of the preexisting RFID technology wherein it combines a smartphone interface and reader on to a single device. It is based on RFID standards namely ISO/IEC 14443 and FeliCa [1].Communication takes place through proximity wave or touch between the devices. In addition to this active transfer, passive communication is also possible using transducers or "tags". The Radio Frequency fields that are emitted from an NFC device act as the power source for NFC tags. Typically, NFC provides a range of around 10cm.

NFC devices can operate in three different modes based on the ISO/IEC 18092, NFC IP-1 and ISO/IEC 14443 contactless smart card standards, namely Read/Write, Peer to Peer and Card emulation. In the Read/Write mode, the NFC enabled phone can read or write data to any of the supported tag types in a standard NFC data format. The Peer to Peer mode allows two NFC-enabled devices to exchange data such as virtual business cards or digital photos. Finally, in Card emulation, the NFC-enabled phone acts as a contactless card or chip-based credit card to a payment terminal or reader.

The Google Wallet application is based on the third mode of operation. It allows users to store their debit cards, credit cards, gift cards [38] and loyalty cards on a smartphone, transforming it into a virtual wallet. Google Offers from participating merchants are also redeemed automatically.

The release of the cloud-based version of Google Wallet [29], extended support to all credit and debit cards from VISA®, MasterCard®, American Express®, and Discover®. This new approach has led to faster technology integration with banks and their associated cards. Moreover, the digital wallet can be accessed from any and all compatible devices, such as tablets, handsets and PCs.

Initially meant to ameliorate the limited choice in credit and debit cards, the Google Wallet Prepaid Card has often been encumbered by security issues. As it is no longer an expedient proposition, it has been phased out on October 17th 2012 [30].

At first the only phone which supported Google Wallet was the Sprint Nexus 4G. Gradually the application was expanded to other phones including LG Optimus Elite, LG Viper 4G LTE, Galaxy Nexus [2], Sprint Galaxy S3 and Nexus 7[3]. All of these are Android phones that carry an embedded chip for NFC. Signals emanating from the device are read at any MasterCard PayPass terminal. As of September 2012, over twenty retail chains accept Google Wallet [33]. The Google Wallet application is designed as an "open" platform. Payment networks, carriers, and banks have been invited to join and participate in the system [15].

In addition to in-store use, Google Wallet has myriad applications that encompass online shopping [25], retail technologies and payment technologies [26].

As of September 2012, the application is free to use [27].

Initially launched only to function in the United States, similar apps are being developed in different parts of the world [4].

2. OPERATION
Google Wallet is designed for easy use on the go, mainly in the domain of customer retail. A user must switch on the display of the mobile device that carries the application. After unlocking the phone, if the user has not entered the application's unique Personal Identification Number recently, then she must do so. Following this, the device must be tapped against a compatible card reader. Payment credentials are then transferred to the merchant. After that, the merchant receives a confirmation on the sales terminal and a receipt is printed, while the customer receives a confirmation on the mobile device. [34]

Cards added to Google Wallet are of two types [31]. Cards such as the Google Prepaid Card and most Citibank MasterCard® cards are directly enabled by the issuing bank for use with Google Wallet. In this case, the use of the application

results in the direct transfer of registered card information to the merchant and the transaction is processed as if the physical card was presented for payment [32].

The addition of other types of cards results in the issue of a "Google Wallet Virtual Card" by The Bancorp Bank. Upon activation, the card is stored in the user's Google Wallet account, which is in turn linked to the user's Google Wallet card. An in-store purchase to a merchant is facilitated via the virtual Google Wallet card and then charged to the selected credit or debit card. In the case of such a transaction, the application presents the virtual Google Wallet card to the merchant, rather than the actual card credentials [32].

Google Wallet stores encrypted user information on a computer chip called the Secure Element. The Secure Element is separate from the phone's main operating system, hardware and memory and uses both hardware and access control. The chip is designed to only allow trusted programs, running on the same device, like Google Wallet to access the information stored therein.

A combination of the PN544 NFC controller along with an embedded SmartMX secure element was chosen for the Google Nexus S. It can also support SWP, which allows a mobile operator put a secure element in the SIM.

Google Wallet makes use of several applets, all pre-installed on the Secure Element. These are described in detail by Nikolay Elenkov [40].

The wallet controller stores information about the current state and timeline of the application. The controller also enables the contactless payment functionality upon unlocking the Wallet app on a user's smartphone.

The MIFARE manager app makes use of an emulated MIFARE chip. MIFARE is a smartcard IC. The manager also uses a log like directory to track added and removed loyalty cards. These can then be retrieved later by tapping at the POS (Point Of Sale).

It is speculated that one or more EMV (Europay, MasterCard and VISA global standard) compatible applets are perhaps used to enable payment with a mobile device at compatible POS terminals.

3. PERFORMANCE

The application is brisk and intuitive. The user does not need to ever launch the application manually and the entire transaction is processed within a few seconds. However, it is not free from payment glitches [11], [12]. It is noteworthy that customers at retail outlets have sometimes received the customary confirmation on the mobile device, but the transaction has failed to complete [10]. But considering the greenness of the application and the fact that credit card payment systems also have a commensurate rate of failure, the performance of Google Wallet is satisfactory.

What is noteworthy is that users of the application have indeed been inconvenienced by remedial measures taken to offset security lapses, although they were compensated later for the same [28].

For now, Wallet is also hindered by the US wireless carrier barrier that prevents users from using Google Wallet on every carrier, but Sprint. [35]

The rival "Isis Mobile Wallet" system, set to launch in October of this year, signed on the three biggest wireless carriers in North America [36], some of which are currently wary about providing the Google Wallet service.

4. COMPARATIVE ANALYSIS

Speaking broadly, three different approaches to NFC based proximity payment solutions exist based on the placement of the secure element. This section compares techniques used by Google Wallet along with other prevailing solutions.

4.1 Embedded Solution

The NFC secure element is embedded into the phone hardware. An example of this is the Google Nexus S.

Benefits:

- Companies like Google prefer that the secure element is embedded on the mobile device so that they have access to customer spending patterns.
- This also allows handset makers to position themselves in a manner that provides easier upgrade paths to newer handset models for customers.
- Secure data encryption during storage and processing along entire data path.

Disadvantages:

- Difficulty in transferring applications to a new handset.
- Not many phones exist currently that support an onboard NFC Chip
- With each new device, applications will have to be retested, leading to delayed deployment.

4.2 SIM based Solution

Traditionally the SIM Card, which already plays a key role on handsets by identifying the subscriber and related account, was the ideal Secure Element of choice for supporting mobile payments. Its formidable security and OTA (Over-the-air programming) provisioning capabilities made it an ideal choice, but ultimately the evolving ecosystem blanched at giving too much control to a single stakeholder – the mobile operator. Control has slowly begun to shift from the mobile operator in to the ecosystem via external SE approaches and Trusted Service Managers (TSM). ISIS, an operator led initiative is a key example of a SIM based SE solution that started its life as an independent payments processor and morphed later in to a TSMix.

Benefits:

- Preferred by organizations and controlled by the issuing party.
- Meets security standards imposed by Financial Institutions
- Faster deployment as this method is independent of handsets, current and future
- OTA(Over-the-Air) Provisioning possible so that new applications can be downloaded remotely
- In the case of a lost device, all applications on the SIM can be blocked (or unblocked)
- Provides mobility for the consumer's financial credentials
- Can be segmented in to a number of security compartments to support multiple cards

Disadvantages:

- When multiple payment applications are present in one SIM card, questions arise as to who maintains control and visibility of credit cards from separate banks.
- Ambiguity around the role operator networks will play in the ensuing transaction and whether they will opt for revenue sharing or a flat fee.

4.3 Secure Digital Card based Solution

This approach commonly comprises of a self-contained SD Card/NFC antenna combo that allows the handset to communicate with contactless readers. DeviceFidelity which provides a microSD card based Secure Element has partnered with VISA on its In2Pay microSD solution to offer NFC payment capabilities across VISA's payWave platform. DeviceFidelity allows its microSD cards to be issued and personalized like traditional smart cards. It has partnered with Vivotech to add OTA provisioning capabilities to its In2Pay microSD product.

Benefits:

- Rapid application deployment
- Works with existing hardware
- Agnostic of operator networks or phone hardware and therefore, preferred by Financial Institutions
- Allows the Card Issuing Bank to own the secure element
- Secure Element can stay in the microSD card while relying on the handset for NFC capabilities.

Disadvantages:

- No standard currently exists on secure communication between SD Card and Keypad/ Screen
- May mean multiple cards for multiple banks
- Requires an available SD Card slot
- Higher Cost and ambiguity over who will pay for the microSD card - customer or the issuing bank

5. VULNERABILTIES AND CONCERNS

A very interesting and pertinent issue for research is the security and privacy concerns that several users, critics and financial institutions have outlined. Many of these raise serious questions about the feasibility of such an application in an area where security is of paramount importance.

To begin with, Android technology itself has proven to be quite vulnerable, it being the prime subject of malware attacks amongst operating systems [24].

A high level forensic security analysis of the Google Wallet application in December 2011 by viaForensics revealed several vulnerabilities in the Google Wallet application [39]. Future versions of Wallet have addressed most of these issues.

Since then, researchers have tried to outline various faults with the Wallet application, particularly the susceptibility to various attacks.

One such attack is called 'fuzzing' [5].In this attack, the application is fed corrupt or damaged data to discover vulnerabilities and to inject crafted NFC tags to a phone and monitor the results [13].

A more serious vulnerability was demonstrated by security researchers at Zvelo in February 2012 [6]. This flaw only affects users who root their Android smartphone. Google Wallet stores a hash of the PIN on the mobile device itself, rather than the Secure Element (SE). PINs were stored as a long integer salt and a SHA256 hex encoded string hash. This allowed the attacker to brute-force against the 10,000 SHA256 hashes of all possible four-digit numbers using the publicly visible salt.

Google recognized that the only way to properly solve the issue would be to move the PIN verification into the secure element itself and no longer store the PIN hash and salt outside the SE. Unfortunately, this would cause banks to become liable for any breaches related to stolen PINs and has hence not been implemented thus far.

After a software update that was released in the same month, a new "Unsupported Device" message [37] is now displayed on rooted devices upon launching Google Wallet. Although the use of the application is still possible, the message stresses the fact that running the application on a rooted device is less secure. Kernel based privilege isolation isn't secure enough to protect sensitive data in Google Wallet, and the use of USB Debugging can still be used to get shell access to the device. Fortunately, the user can avoid the use of both these features for extra security.

Not surprisingly, individuals have found a way to infiltrate an unrooted device too [8]. In the same month, a glaring security hole discovered by a user demonstrated how an individual with access to your phone needs to simply clear data in the app settings to enforce Google Wallet to ask for a new PIN. Once a new PIN is entered Google Prepaid cards which were being used by the owner of the phone can be added thereby allowing easy access to all available funds. The flaw here was that the funds of a particular account are linked to the mobile device itself and not to the Google Account.

Responding to the security lapse, Google temporarily disabled the provisioning of prepaid cards within days of the news [14].

The issue was fixed within a week by a software update that prevents an existing prepaid card from being re-provisioned to another user [14].

Privacy concerns include the storing of data regarding payment information, transaction details, payment attempts and other information stored by Google indefinitely. The Privacy Policy for Google Wallet indicates that much of the data is stored but may not be shared outside Google except under certain circumstances [22].

6. POTENTIAL ATTACKS AND DEFENSE FROM AN NFC PERSPECTIVE

At the centre of the Google Wallet system is an NFC enabled smartphone, hence it is obvious that all the vulnerabilities pertinent to NFC are also relevant for Google Wallet. NFC provides a wide entry point for several attacks and hence it is no surprise that individuals have found ways to exploit the use of this technology and its underlying protocols.

Charlie Miller, through his research at Accuvant has exploited multiple security vulnerabilities in secure NFC devices [7]. Miller demonstrated how to use NFC to establish a Bluetooth connection between a handset and his laptop, exploiting the fact that some NFC enabled phones accept all connection requests without prompting. He also used crafted tags to take control of the application daemon that controls NFC functions

and exploited peer to peer data exchanges to force a handset browser to open and navigate to as he pleased.

The sanctity of the secure element has also been the subject of scrutiny in research. As demonstrated by Roland, Langer and Scharinger [21], a secure element may not be sufficiently protected on certain device platforms, particularly when the underlying operating system and hardware cannot be fully trusted. In their paper, they illustrate several attack scenarios where the protection mechanism of an API (Application Program Interface) for secure element access can be circumvented for malicious usage.

Another problem in wireless payment applications is eavesdropping. In this attack, data which is stolen wirelessly is used to clone magnetic stripe cards [9].

In 2006, Ernst Haselsteiner and Klemens Breitfuß described several possible types of attacks [20], including modification of data transmitted via the NFC interface (data corruption), modulation of signal being received to create valid but manipulated data (data modification) and data insertion between messages. In their paper, they also detail how to leverage NFC's resistance to Man-in-the-middle attacks to establish a specific key.

Solutions to NFC based attacks are few and far between. Haselsteiner and Breitfuß recommend several strategies from eliminating response delays to periodically checking the RF field.

However, as noted by the same two researchers, establishing a secure channel between two NFC devices is by far the best approach to protect against eavesdropping and any kind of data modification attack. For Man-in-the-middle attacks, they suggest the use of an active-passive communication mode such that the RF field is continuously generated by one of the valid parties. The active party can then listen to the field in order to detect any disturbances caused by an intruder.

Miller through his research has found that in order to exploit the avenues of attack, the attacker must get close enough to an active phone to prompt an NFC action to occur. Further, attacks would require the screen to be on and in some cases the device would have to be unlocked.

7. SECURITY SAFEGUARDS IN GOOGLE WALLET

In addition to the software updates and fixes described in earlier sections, Google Wallet Application provides security at several levels [16], [17], [18], [19].

When the screen of the phone is off, the transmitter chip is not powered and therefore stores no data. This prevents the skimming of data by a passing hacker. Moreover, if the application is locked (either manually or automatically after a few minutes), a 4-digit Personal Identification Number is required to view and use cards that the virtual wallet contains. Upon completion of the transaction, the antenna of the NFC chip is turned off. Additional transactions require the PIN to be entered again to power the chip.

In the event that his or her mobile device is lost or stolen, the user can remotely disable the Google Wallet account online. Upon connecting to the device, Google Wallet will remotely reset the application, clearing all payment and transaction data. This prevents the use of the phone for any unauthorized purchases.

Google assigns each Wallet user a unique Mastercard credit card number, which is used to make the transaction regardless of which stored card you select. However, prepaid cards and Citi Mastercards are still stored in the Secure Element part of the device.

Instead of storing linked debit or credit card credentials on the secure element, the application now stores the same on Google servers and only stores a wallet ID on the phone. Hence the real credit card numbers are usually masked ensuring a more secure transaction.

8. FUTURE PROSPECTS

Several additions can be made to make Wallet more expedient to users. The added functionalities suggested here are aimed at extending usability, increasing the customer base and enabling cross compatibility.

It is notable that the most successful mobile payment system in the world is M-Pesa, operated by Safaricom and Vodacom in Kenya and Tanzania [42]. The most developed mobile payment system in the developing world has over 17 million users and is used to send balances using SMS technology as well as to redeem deposits for regular money.

Wallet's association with Paypal can be used to enable person to person payments along the same lines. This can go a long way in increasing the application's popularity.

The system of loyalty cards that Google uses in conjunction with store outlets has also not been fully exploited. Expanding the tools with which stores can create their own loyalty cards can aid both in the personalization of payments and is likely to contribute to an increase in customer loyalty.

Wallet can also be used in conjunction with public and private transport systems. The use of various transit cards can be linked with wallet allowing the user to quickly and efficiently pay for her travels.

Google briefly displayed information about "Eligible devices for use with Google Wallet card" on their help website. Though this was later taken down, it is likely that there will be a paradigm shift in the mobile payment system. Physical card technology would allow Google Wallet to become usable in any store that accepts credit cards. Moreover, the application would not have to be tied to phones that use NFC or to the Android operating system. This would pave the way for compatibility across store outlets and mobile platforms. The use of a physical card could also serve as a backup for a battery-dead phone and could be disabled by the mobile device itself in case it was stolen.

On the security front, Google announced that it will use fingerprint sensors as an added security measure [43].

A comparative analysis of attacks shows that users are most vulnerable to attackers who they are acquainted with or those who can get within close proximity to their mobile devices. If an attacker was to put a device next to an NFC payment terminal or use some kind of antenna across the room then the user's device can be susceptible to a hack.

If the victim is known to the attacker, simply making a call or sending a text message ensures that the victim activates the mobile device.

In the future the application would do well if it ameliorated concerns in these respects.

9. CONCLUSION

In concluding this paper, an attempt is made to understand if and when applications like Google Wallet will be able to permanently replace cash and card as a means of payment.

Miller notes that any time a new way for data to enter a device is added, it opens up the possibility of remote exploitation by an attacker. He concludes his literature by saying that the new attack surface introduced by NFC is large and the opportunity to exploit it extends from kernel drivers to end applications.

As it stands, the Google Wallet application is circumscribed by inherent problems that are not encountered by traditional payment methods, such as the unreliable battery life of today's smartphones, an operating system that can hang or crash and lack of resistance to physical elements, particularly water. These are, of course, in addition to the issues already highlighted in this paper.

Equally questionable is support for NFC enabled payments in America. The launch of Isis has been delayed several times [41]; the most recent postponement came shortly after the debut of iPhone 5, which did not have NFC functionality. The fact that a market leader like Apple has still not supported this technology in their products lends credence to the possibility of a slow adoption in the United States. This is in stark contrast to Japan, which has had mobile payment services for years.

The benefits of the system however, are far reaching. Service providers in America have long said that they are keen to support mobile payments to help improve their customer loyalty. In the mobile payment system, credit card companies receive a percentage of payments; terminal companies improve product sales and Internet companies are able to gather valuable customer data. This is in addition to the rather obvious benefits to customers and partnering merchants.

Applications like Google Wallet hold tremendous potential and can potentially revolutionize traditional payment methods. But whether such systems are infallible, is a question that is still open for debate.

10. REFERENCES

[1] RFID standards used by NFC: "Technical specifications" NFC Forum.retrieved

[2] Phones supporting Google wallet: "Google wallet Google + post." Retrieved

[3] Phones supporting Google wallet: "Sprint Galaxy S III arrives with Google Wallet on June 21 post". Engadget. June 4, 2012. Retrieved June 4, 2012

[4] Ross, P.E. SPECTRUM IEEE Volume: 49, Issue 6 Digital Object Identifier: 10.1109/MSPEC.2012.6203971 Publication Year: 2012, Page(s): 60 - 63

[5] What is Fuzzing?: http://www.americanbanker.com/issues/177_138/google-wallet-still-dogged-by-security-perception-1051012-1.html?pg=2

[6] Vulnerabilities demonstrated at Zvelo: http://zvelo.com/blog/entry/google-wallet-security-pin-exposure-vulnerability?q=/blog/entry/google-wallet-security-pin-exposure-vulnerability

[7] Security Vulnerabilities at Accuvent: http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf

[8] Attack on unrooted devices: http://thesmartphonechamp.com/second-major-security-flaw-found-in-google-wallet-rooted-or-not-no-one-is-safe-video/

[9] Eavesdropping attack: http://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/

[10] Customary failure of transaction completion: http://rootzwiki.com/topic/31572-google-wallet-failed-transactions/

[11] Payment glitches in the application: http://support.google.com/wallet/bin/answer.py?hl=en&answer=1349471

[12] Payment glitches in the application: http://support.google.com/wallet/bin/answer.py?hl=en&answer=43068

[13] Fuzzing attack procedure: http://mcafeesecurity.org.uk/misc/mcafee-warns-on-olympic-nfc-fraud-risks.html

[14] Temporary disabling of prepaid cards provision: http://googlecommerce.blogspot.in/2012/02/protecting-your-payments-with-google.html

[15] Which mediums have been invited to associate with the system?: http://techcrunch.com/2011/05/26/google-wallet-offers/

[16] What are the security safeguards used?: Le, Tony (June 1, 2011). " Google Wallet FAQ". GFan. Retrieved June 4, 2011.

[17] "Engadget Primed: What is NFC, and why do we care?" Engadget Retreived June 22, 2011

[18] What are the security safeguards used? :"Google Wallet Security". Google. Retrieved June 22, 2011

[19] What are the security safeguards used?: "MasterCard PayPass". MasterCard. Retrieved June 22,2011

[20] Attacks decribed by Haselsteiner and Klemens: http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf

[21] Practical Attack Scenarios on Secure Element-enabled Mobile Devices-Michael Roland, Josef Langer and Josef Scaringer.

[22] Google Wallet :Privacy Google Retrieved September 20, 2011

[23] Google wallet launch: http://googleblog.blogspot.in/2011/09/launching google-wallet-on-sprint-and html

[24] Susceptibility of android to malware: http://www.ieee-security.org/TC/SP2012/papers/4681a095.pdf

[25] Google wallet applications: http://www.google.com/wallet/how-it-works/online.html

[26] Google wallet applications: https://developers.google.com/commerce/\

[27] Google wallet free to use: http://www.google.com/wallet/faq.html

[28] Compensation for application users: http://www.droid-life.com/2012/03/20/google-wallet-team-you-can-add-prepaid-cards-again-we-tossed-in-5-to-apologize-for-the-last-few-weeks/

[29] Cloud based version of Google wallet: http://googlecommerce.blogspot.in/2012/08/use-any-credit-or-debit-card-with.html

[30] Phasing out of google wallet prepaid card: https://www.google.com/wallet/prepaid-refund/

[31] What type of cards are added to Google wallet?: http://support.google.com/wallet/bin/answer.py?hl=en&topic=1349429&answer=2701024

[32] Direct transfer of registered card information: https://wallet.google.com/termsOfService

[33] Retail chains shops accepting Google wallet: http://www.google.com/wallet/how-it-works/in-store.html#merchant-matrix

[34] Operation of Google wallet: http://www.google.com/wallet/how-it-works/

[35] The only carrier using Google wallet currently: Sprint http://www.google.com/wallet/current-partners.html

[36] Wireless carriers signed by ISIS mobile payment system: http://www.paywithisis.com/get-isis.xhtml

[37] What is "unsupported device message"?: http://www.droid-life.com/2012/03/05/google-wallet-now-showing-as-unsupported-on-rooted-devices/

[38] Cards stored in Google wallet: http://support.google.com/wallet/bin/answer.py?hl=en&answer=1611356

[39] Vulnerabilities in the application: https://viaforensics.com/mobile-security-category/forensics-security-analysis-google-wallet.html

[40] Applets used in Google wallet: http://nelenkov.blogspot.in/2012/08/exploring-google-wallet-using-secure.html

[41] Why launch of ISIS has been delayed?: http://uk.reuters.com/article/2012/09/13/business-us-mobilepayments-isis-idUKBRE88C1CN20120913

[42] Jack, William; Suri, Tavneet (August, 2010). [www.mit.edu/~tavneet/MPESA.pdf The Economic of M-PESA,]Change

[43] Google unveils safety measure for their upcoming mobile wallet: http://www.qrcodepress.com/googleunveils-safety-measure-for-their-upcoming-mobile-wallet/853399/