Locking down the e-wallet


Tracey Caldwell

Tracey Caldwell, journalist

The Google Wallet mobile app made the e-wallet concept mass market, but security breaches were not far behind.

The emergence of near field communications (NFC) and other contactless technologies in mobile devices represents a step towards the elimination of cash. With a recent Juniper research report indicating that NFC payments are set to triple by 2015, and over $74bn-worth of contactless transactions expected in three years, organisations are keen to ensure they are able to offer a secure mobile payments solution to meet customer demands.

Richard Cottrell, sales and marketing director at Vista Support, describes a cashless society where restaurants, for example, are enabling automated ordering and payment from the table. NFC can speed up the painful bill splitting process by allowing the each member of the party to transfer their part of the bill to one other through their smartphones, therefore making it possible for the bill to be settled by one person.

"Technologies like this are enabling the move towards a cashless society and with developments like Google Wallet already being used, this may not be far away," says Cottrell. The Google Wallet mobile app claims to not only store credit cards on the phone but also retailers' discounts and offers, as a loyalty card would. When a person checks out at a brick-and-mortar store that accepts Google Wallet, he or she can pay and redeem offers just by tapping the phone at the point of sale. The Google Wallet online service enables people to pay by signing into their online accounts, and credit cards details are stored in the cloud.

Google wallet bypass

However, according to recent reports, the PIN authentication in Google's e-wallet has been bypassed using a simple trick. H-Online reports that an attack on Google Wallet's PIN protection, which required that the phone be rooted so that the PIN information could be accessed, can be achieved on an un-rooted Android smartphone by using a Linux privilege escalation vulnerability.

Rooting would usually mean that all the data on the device was deleted in the process and Google advised users not to use Wallet on rooted devices. But by exploiting a Linux privilege vulnerability in Android 4.0, it is reportedly possible to get root access to the device without deleting any data. Web categorisation company Zvelo, the company that found the vulnerability, says this is enough to get access to the Google Wallet PIN data, which can be easily brute-forced. An attacker could also just obtain the data and send it to a remote server where the PIN could be brute-forced even faster.

Standards for security

That flaw has now been fixed but security concerns remain. "One of the main reasons why the Google Wallet was susceptible to brute-force attacks was that its design seemed to be based on proprietary technology instead of recognised standards and processes. Although the mobile security market is rapidly evolving, there does exist a set of standards that e-wallet developers can use to make apps more secure," says José Díaz, director, technical and strategic business development at Thales e-Security.

"One of the main reasons why the Google Wallet was susceptible to brute-force attacks was that its design seemed to be based on proprietary technology instead of recognised standards and processes"

In today's smartphones there is a separate chip called the Secure Element. Apps that use the Secure Element to secure their critical operations will be difficult to compromise but interacting with the Secure Element can be an issue for developers. That's why the SIM Alliance developed the Open Mobile Application Programming Interface (API). The API provides app developers with a common interface to make better use of the Secure Element for their apps, including e-wallets.

Díaz points out that the Secure Element, however, is not an environment that can run an e-wallet with a cutting-edge user interface. If a developer wants an e-wallet with a rich user experience, the e-wallet app must run in the operating system. "The Trusted Execution Environment (TEE) is designed to secure apps that function in this way and GlobalPlatform is leading the way for standardisation and interoperability in this area. An e-wallet which runs its transaction security in the Secure Element and its user interface in the TEE would be very difficult to compromise," he says.

Díaz adds: "E-wallets are beginning to take off as they are an attractive payments

The C-mii phone allows users to pay for goods and services using NFC technology.

option for consumers. 'Tap and pay' is a far easier way to make purchases than inserting a card into a point-of-sale, entering a PIN and waiting for the transaction to be authorised. Yet, if this convenience is not supported by robust security, e-wallets will never become mainstream. Mobile payments is an evolving market and we are learning much from the early adopters, which will help us shape not only the products which are offered but also the required security for consumer confidence."

The threats

Gary Clark, VP EMEA at SafeNet, outlines the threats to e-wallet security: "Sophisticated threats like Man-in-the-Browser or Man-in-the-Middle attacks can easily intercept online transactions by reading payment data from the Internet browser while the user is typing his credit card or bank account details," he says. "What's even more alarming is that common threats such as phishing attacks or social engineering can be used to steal users' login details and personal data, making online payment accounts susceptible to fraud."

He believes online merchants and payment providers need to take responsibility for putting the right systems in place to safeguard user privacy and authenticate online transactions. "Encrypting all user data, not only payment details, is the first step to ensuring e-wallets are protected. Another important factor is using advanced authentication solutions for large money transfers that can verify not only the user but also the validity of the online transaction," he says.

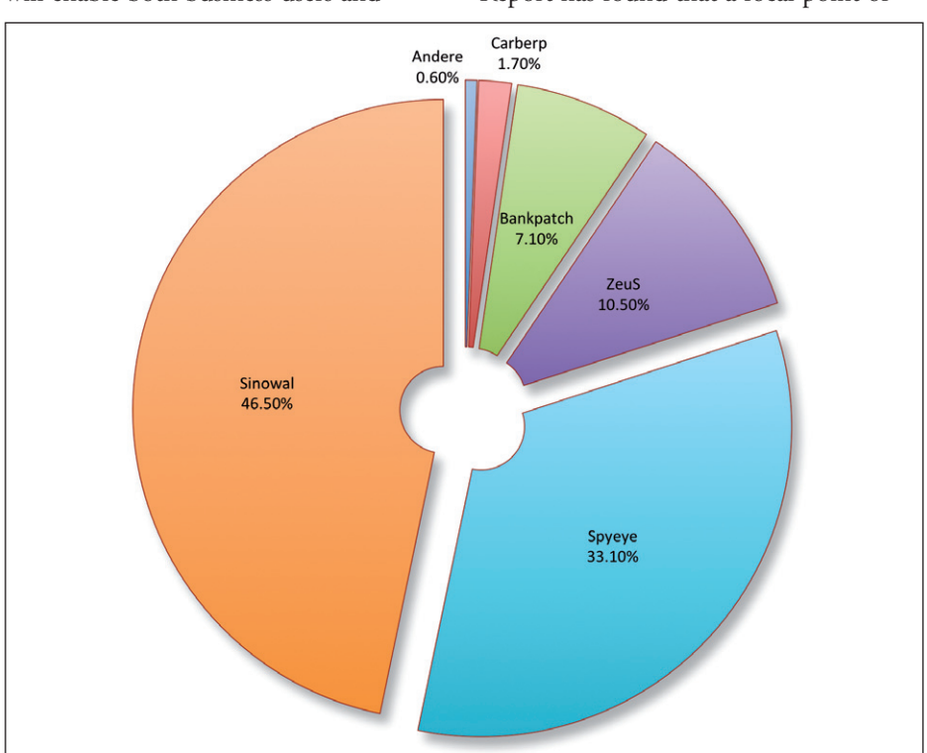
Tokens that use optical sensors to read data from the screen and generate unique electronic signatures to validate each transaction are a good defence against Man-in-the-Browser and Man-in-the-Middle attacks, according to Clark. Using optical tokens prevents hackers from interfering during online payments and redirecting funds to fraudulent bank accounts. Another benefit of this approach is that it allows online payments to be verified against the customer data stored with the bank server, thus reducing the possibility of transaction tampering and payment fraud.

Limited risk

Chris Pay is CEO of PayFones, which is launching a range of NFC-enabled mobile handsets called C-mii that will enable both business users and consumers to pay instantly for goods in shops, restaurants, transport hubs and many other locations. The devices look much like standard mobiles and perform many of the same functions, but are equipped with near-field tag reading components that allow simple transactions from a linked bank account to be completed very quickly and without direct contact.

Pay points out the current limit on e-wallet payments limits risk: "The most important reassurance is that we are talking here about 'micro-payments'. Currently, an individual's mobile payments in the UK are statutorily limited to £15 per transaction, although this is likely to rise shortly in line with the €70 limit that is applied in most parts of Europe. In the event of a C-mii phone being lost or stolen, the owner could contact his or her service provider and it would be shut down very quickly. He adds: "It's also important to point out that the device itself does not allow the user access to personal banking information. It simply facilitates and logs small everyday transactions."

The G Data bi-annual Malware Report has found that a focal point of



Banking trojan families detected by G Data in the second half of 2011.

malware writers seems to be banking trojans that attack the highly secured connection between the bank and the user.[1] Analysis shows that the interval between new trojans being launched at online banking customers is decreasing steadily. With an average lifecycle of 27 hours, malware authors try to circumvent reactive defence mechanisms in antivirus software.

"There are a select few families of banking trojans, and these are used as the basis for constantly creating new malware variants with ever-shorter lifecycles"

Eddy Willems, G Data's security evangelist, says: "We've been seeing a rise in bank trojans that can break into secure online banking sessions. The lifecycle of these highly intelligent malware is getting shorter, and is now only around 27 hours. Online banking is a popular service that more and more people are using. As with other services, increasing user acceptance has also made it more appealing to cyber-criminals. Cyber-criminals use special banking trojans to manipulate online banking transactions, for example, in order to transfer specified monetary amounts to other accounts."

Analysis by G Data SecurityLabs reveals that there are a select few families of banking trojans, and these are used as the basis for constantly creating new malware variants with ever-shorter lifecycles. This tactic seems very effective, as a study by the Bonn University and G Data SecurityLabs shows that the detection rate within the first 24 hours of new banking trojans by the 43 top-selling virus scanners averages at 27%.

Plugging security holes

Dale Gonzales, product strategist at Dell SecureWorks, says: "There are measures that can be introduced to limit the risks that consumers face from e-wallets. A good authentication mechanism can

Dale Gonzales, Dell SecureWorks.

be integrated into a mobile handset to make it difficult for criminals to access the device but easy for the mobile user to unlock it and use it. A Trusted Platform Module (TPM) would help in that situation. A TPM stores cryptographic keys to protect personal information such as credit card numbers and passwords."

The major risks to e-wallet security are not all technology-based. Gareth Maclachlan, COO and co-founder at AdaptiveMobile, explains: "Security risks from e-wallets or mobile wallets emerge when users often forget to wipe the device clear of sensitive information such as credit and debit card details, PIN numbers and bank account details. If a mobile or electronic device falls into the wrong hands, then this type of information can easily cause a lot of financial damage to the previous owner. However, the biggest risk from e-wallets arises when criminals execute scams or frauds which trick or coerce users into either unintentionally revealing their personal information or clicking links which appear to be genuine, but are in fact built with the sole purpose of defrauding users. This risk is particularly strong with the use of mobile wallets as consumers are more likely to fall prey to these threats on a mobile phone, rather than a PC due to the personal nature of the mobile device, meaning any communication to these devices is typically more trusted."

Maclachlan adds: "The attractiveness of mobile devices to hack, scam and defraud is only going to increase as the adoption of mobile wallets continues to increase and our mobile devices become heavily linked to funds or credit."

He points out that to complicate matters, no one really owns the security for mobile banking, as it is an issue shared by banks, mobile operators, and credit card companies, each of which has its own ideas of what constitutes good security measures.

Role for retailers

Some observers believe retailers will drive e-wallets in the UK, possibly resulting in a strong, standardised infrastructure. Retailers are showing increasing interest in linking e-wallet apps with loyalty and coupon features. However as loyalty and 'couple apps' are increasingly linked with social networking sites – where friends share information about purchases – and location data, the security threats would appear to multiply.

Analyst firm Frost & Sullivan expects joint ventures and collaboration among market participants will be key market drivers for the mobile payments market. It believes joint ventures established between major telecom operators and financial institutions will drive the market.

"With joint ventures, market participants can leverage their brand name across diverse industries to create awareness of m-payment services," says Frost & Sullivan research analyst Jayashree Rajagopal. "Similarly, regional factors such as the level of credit/debit cards usage in a particular country have to be considered when developing alternative payment services aimed at increasing customer adoption."

He adds that, although a number of partnerships have been announced, business models have often not been clearly defined due to issues such as revenue sharing requirements and that the fragmented approach of market participants has resulted in low awareness of m-payment services.

This would not appear to bode well for concerted efforts on security.

Role of merchants

In order to overcome security threats, businesses would do well to learn from the finance world, according to Russell Sheffield, director of innovation and development at Paythru. The Payment Card Industry (PCI) has a long history of ensuring the financial security of payment systems through best practices such as PCI DSS compliance, and mobile commerce needs similar standards to fully develop and foster consumer trust. "The ultimate aim is Level 1 PCI DSS compliance, the highest security standard that the card issuing schemes rely upon. This level of compliance should also co-exist with other technologies to combat other common fraud risks such as cardholder-not-present or card cloning," says Sheffield.

Mobile payments should evolve beyond e-wallets and NFC, which have limitations, Sheffield believes. "Ultimately, mobile payments should be universally available across any device, on any network, from any location for it to really take off."

Roelant Prins, chief commercial officer at Adyen, provider of an Internet payment system for international merchants, says: "The success of an e-wallet lies in ease-of-use [that] typically conflicts with security requirements, so it is vital that merchants running an e-wallet infrastructure ensure that they have the best possible data security measures in place. The payment system needs to be PCI compliant and a high degree of fraud control is essential. Specialist payment service providers, offering a hosted service that removes these burdens from the retailer, can often be the easiest route to do this."

Security in the cloud

Moving e-wallet security into the cloud could address some of the issues of on-device security. Thomas Bostrøm Jørgensen, CEO of Encap, provider of software-based, two-factor authentication and digital signing for the enterprise and banking sectors, says: "E-wallets are the next big thing. The Google Wallet, for example, is a 'poster child' for NFC-based m-commerce. As such, they face a greater level of scrutiny and attack. Education and marketing around the security of these services, in particular, will be vital in driving consumer adoption."

He adds: "The recent Google Wallet attack was described as 'theoretical', but it has driven fear, uncertainty and doubt in the minds of consumers around the world. But we must remain confident in mobile – it offers the solution to many security problems, if done correctly. For example, by performing PIN authentication in the cloud, susceptibility to 'brute force' attacks can be avoided."

Independent e-security solutions expert Cryptomathic has launched its 'Cloud Wallet' that enables a secure payment application to run off a connected, trusted platform accessible through the Internet. It links users and all their devices – such as smartphones, tablets or personal computers – securely to their wallet.

Cryptomathic is marketing this as an alternative approach to providing secure payment applications, which today are generally delivered through either EMV chips embedded in payment cards or secure elements of smartphones.

User awareness

Many of the security challenges and solutions around e-wallets are not new. Steve Durbin, global VP at the Information Security Forum (ISF), says: "NFC, which is essentially powering e-wallets, has been around for a while. Nokia was shifting phones with NFC years ago, so there's nothing new there. But NFC itself is not a secure technology: it requires encryption, anti-virus, malware protection, authentication, so when people talk about NFC they sometimes assume all of these things are already there. Not necessarily."

Roelant Prins, Adyen.

Durbin believes there is no substitute for security awareness among mobile phone users. "Mobile wallet, and the potential for theft and hacking, hits the user fairly and squarely between the eyes, so they need to be sure that they are taking the necessary precautions when using NFC, but also taking care of the physical safety of the device. Things like password protection, keypad locks, etc all become essential to protect against theft and abuse of the NFC-enabled device. Training users in this way is always the biggest challenge," he says.

Conclusion

Some 70 million people in India now use mobile payments, according to the 2011 Indian survey. E-wallets have high adoption rates in developing countries and look set to become established worldwide. The challenge of ensuring security may well affect how far the e-wallet becomes part of all our daily lives.

About the author

Tracey Caldwell is a freelance business technology writer who writes regularly on security issues. She is editor of Biometric Technology Today*, also published by Elsevier.*

References

1. 'G Data Malware Report: Bi-annual report July-December 2011'. G Data SecurityLabs. Accessed March 2012. www.gdatasoftware.co.uk/uploads/media/GData_MWR_2_2011_DE_EN_final2.pdf.