December 2012

VECTOR

A Net-Square Initiative

A series of articles specially designed for the information security professionals.

Mobile Wallet ≈ A Hole in the Pocket

Technology follows Life. And just as in life, there is good and bad with every technology. Everybody will agree that Mobile technology came and changed the entire communication landscape and did a lot of good. In its second avatar now, the Smartphone radically changed how people interacted whether for business or for pleasure. Blackberry changed the way people collaborated for business through e-mail and iPhone, and the likes, changed the way we searched and socially interacted with others.

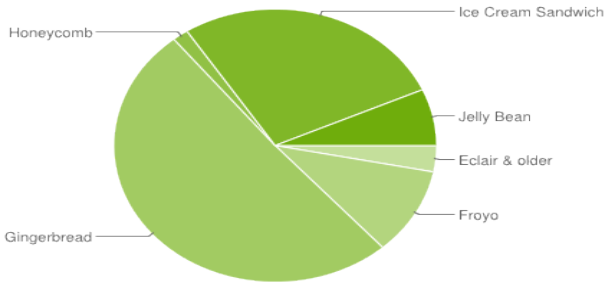
A little talked about fact is that Mobile technology has also been very effectively utilized by Financial Sector Enterprises to provide additional security to their customers. Mobile technology became a great **"Out of Band" Authentication** tool. By definition, Out-of-Band Authentication is the use of two separate networks working simultaneously to authenticate a user. Until mobile technology was adopted for "Out of Band" authentication, most authentication was done using the approach of a token (what the customer has) + a pin (what the customer knew). Technically both were part of the same infrastructure and therefore if the network or infrastructure was compromised, so were both these controls. Case in point – Lockheed Martin's RSA token compromise.

Mobile technology provided a dynamic generator of 2nd factor of authentication, which was a pure out of band implementation – not hosted in the infrastructure of the Enterprise. "One Time Passwords" (OTPs) sent out on a mobile device every time a transaction has to be done by the customer is an example of a pure out of band 2nd factor authentication. ***So in some ways mobile devices became the last bastion in securing financial transactions.***

With the advent of smartphones and Mobile wallets, the ugly side of mobile technology will now rear its head. Financial Institutions and Mobile Companies have effectively transitioned mobile devices from being an out-of-band security device to a financial store itself. Its implementation leaves me convinced that it could definitely hasten the next wave of attacks on mobile devices and mobile operating platforms. Mobile wallets are being designed to especially benefit the less literate and hasten the process of getting them into the main stream Financial System.

Today more than 68% of the smartphones are running on the Android platform. Out of these, the majority are running Android versions Gingerbread and Froyo. These are old, outdated and vulnerable versions of the Android OS.

Diagram: Distribution of Android Operating Platforms



Source: http://developer.android.com/about/dashboards/index.html

The fundamental reason behind this is that the earlier versions of Android based smartphones were largely made and sold by third party mobile phone companies like LG, Samsung etc. It implies therefore for every Android update published by Google, the smartphone maker would have to follow it up with its own device specific update and push it to the phone. As a result, phones stay unpatched, leading to thousands of malwares mushrooming on Android platforms, especially the older versions.

continued.....

Hiren Shah
President, Net-Square
reach him at hiren@net-square.com

Secure • Automate • Innovate

Net-Square Solutions

is a niche Application and Network Security Service provider. Net-Square provides Consulting Services like Vulnerability Assessment, Penetration Testing, Code Review, Reverse Engineering and Security Architecture Consulting

Net-Square also offers Product like Server Defender Vulnerability Protection (SDVP), a web application Firewall for IIS applications and NS Webscan, an automated application vulnerability scanner

Last but not the least is the training programs. Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~*Breaking*~~ *Hacking News:*
Minister's website defaced by hackers!

In a recent news article, it was reported that Indian IT Minister Kapil Sibal's website was defaced by members of Anonymous Group.

This highlights the extent to which hacker and activist groups are able to strike at will whenever they wish.

To read more visit :
http://timesofindia.indiatimes.com/topic/Kapil-Sibal%27s-website-hacked

Continued from earlier page:

According to one of the Anti-virus firms, the number of malwares on Android rose from 4,900 to more than 28,000 in the past year. Couple this with the fact that the only control in place on inter mobile wallet fund transfer is a mere four-digit Mobile PIN! Yes, you read that right. The only other feature, which is arguable whether it's a control, is a confirmatory SMS delivered to the phone when a transaction is performed.

Do you see a problem? Consider this scenario:

An attacker creates a malware bundled in a free app or game and hosts it on a 3rd party store or website. A large number of users would be tempted to download and use it. The attacker gathers information about the usage of the mobile phone. When the victim is uses a mobile wallet service, the attacker collects a lot of important information including the MPIN. The attacker then triggers the malware to transfer the money to their own mobile wallet account at the right moment and subsequently erase the confirmatory SMS. The victim will not even realize that the money is gone. Indian Telcos have established transaction limits as high as Rs. 50,000/- per day for transactions to registered merchants! Today, anyone can be a registered merchant – a Paan/Cigarette/Convenience Shop, an Internet Café or a General Provisions Store. Imagine a mobile user in Mumbai losing her money through payments transferred to a cigarette shop in Chennai! How would law enforcement agencies ever be able to track down such complaints! Unlike banking frauds, mobile wallet frauds will involve small amounts in individual cases but large volumes. I can see law enforcement agencies overwhelmed with mountains of small cases trying to track down and recover money for the hapless users whose mobile phones have been hacked.

Mobile devices are the out-of-band 2nd factor authentication mechanism for desktop based Internet Banking. But what serves as the out-of-band 2nd factor authentication mechanism for mobile wallets? Currently the mobile payment service does not involve any secondary check. Mobile payment companies will have to think up of a 2nd factor authentication mechanism for mobile payment. That could be printed grid cards, tokens or OTP cards or something that the individual knows.

There are other ways for mobile payment companies to rein in frauds. They can use the fraud detection techniques like the ones typically used by credit card companies. In the above example, why should a person in Mumbai want to make a mobile payment to an cigarette shop in Chennai? Such transactions could be followed up with an "out of wallet" security question that must be correctly answered, from a list of questions provided at the time of registration.

Another aspect of Mobile wallet on which needs to be urgently clarified is that about handling customer complaints of unauthorized mobile payments. Early signs of these troubles are already emerging in Kenya, one of the biggest mobile payment markets. Many merchants in Kenya are refusing to join the Mobile payment system fearing payment reversals by the mobile companies upon vociferous complaints from the customer. The fundamental problem lies in lack of clarity around assigning responsibility.

The Reserve Bank in India and equivalents other countries shall have to seriously consider all of the above issues. It is about time that they produce clear, exhaustive guidelines for Mobile Wallet service providers. These services are equal to those provided by Banks or Financial Institutions. The guidelines need to explicitly spell out minimum-security requirements for any Organization planning to offer Mobile Wallet services, including handling of customer complaints. These guidelines should subsequently apply to any application which use mobile devices as a medium to transfer funds. Time has come to take a holistic look at the use of mobile wallets as an alternative to cash or plastic. After all, the last thing one wants is a hole in their pocket!

- Hiren Shah, President, Net-Square

"Smart" Phones ≠ "Smart" Security: Part 2

With cyber attacks increasingly targeted at smart phones and mobile malware increasing year over year at a rate of 250%!, it's a tough job for CISO to shape and control mobile device security. So in continuation of my July 2012 article on "Smart Phones ≠ Smart security", the second and final part focuses on a few pointers that CISO's can follow to tighten smart phone security.

Mike Stramaglio, President and CEO of MWA Intelligence, writes in an article on theimagingchannel.com, that out of all the security threats, Web Browsers on smart phones stand out as a key security risk. Mobile applications rely increasingly on the web browsers, thus making smart phones soft targets for major data thefts. Cyber attacks now a day are no longer restricted to a particular smart phone or operating systems. MobiThinking, a leading mobile internet services company, in its April 2012 report stated that last year malware targeted at Android phones infected more than 250,000 users and a single hacker stole data from more than 100,000 iPad users. An October 2012 survey conducted by TNS Omnibus on behalf of security firm Sophos Ltd. revealed that 1 in 5 of the lost smart phone devices had access to owner's work email, and with poor passwords and PIN codes it was potentially exposing confidential corporate information!

As the market for smart phones grows by 29.6% CAGR and with the mobile application developers still trying to securely code and patch their applications, it becomes important for the CISO of the company to focus on secure utilization of the mobile device.

A way to bring down the risks includes formulating a new IT security strategy where mobile security strategy is independently drafted. This should be reviewed every 6 months. CISO's need to strictly implement basic things like how long passwords should be and setting of time duration before a device locks out. There should be security controls across various mobile platforms to manage access of emails and data. In case a mobile device is lost, there should be a web-based portal, which helps to remotely lock the device and if need be purge the device of all the information. Instead of using smart phone's web browser, user may use application specific utilities built by trusted companies. Lastly, User training on social media and secure web utilization will go a long way in ensuring mobile security!

- Hardik Kothari, Manager Client Acquisitions & Client Relations