May-June 2013

V e c t o r

A Net-Square Initiative

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

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 Products 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, Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

Breaking News:

Net-Square is empanelled with CERT-In!
Net-Square has added a new feather in its cap! The Organization is empanelled by CERT-In for providing information Security Auditing Service.

Cert-In, which is the Indian Computer Emergency Response Team, is the national nodal agency for responding to computer security incidents when they occur.

The Full Picture

Before I start off with my article, let me apologize for not keeping the date for the May 2013 Vector. As we embarked on our new journey of growth in Net-Square, I half expected a period when operational matters will impinge on our time of thought leadership and that happened in May and June 2013. In a way it is a good problem to have and we are now over that hump so we are back on track with our thought leadership. To make up for it June Vector carries more content than normal. Now on to "The Full Picture"

At the outset, let me apologize for repeating an issue. That too in two consecutive articles. But after my piece in the April 2013, I came across business process, which has compelled me to make my point stronger and probably look at the issue more holistically. In April 2013 issue of Vector, I wrote an editorial titled "Sometimes it's about the functionality also…" in which I highlighted that security is not always a function of technical flaws but also how functionally the application is structured. I have to now submit that security issues go even beyond the functionality of the application. Let me highlight that with a real life example. It is from India so my non-Indian friends, if you have any questions on it, I will be happy to answer them.

For my recent visit to Europe, I needed to carry some Euros with me. As we all do these days, I opted for a prepaid forex card. I went to this very well known Bank that offered me the best forex rates. The process was as follows:

- I was asked to sign a request form for the amount of euros required by me and mention my account number, which should be debited for the transaction. And I was asked to provide copy of my passport and visa. I asked if they needed a cheque from me and the executive said "No", just mention your account number. No requirement for me to provide a specific cheque. I found this strange as when I request for a draft I need to give a cheque along with the draft request form.
- After I signed the request form, my sign and the account were checked by the executive and in some time he got me an envelope.
- The envelope contained a chip ATM VISA card with the words "EMV EURO" inscribed on it. There was also a secondary card in the envelope, which I should use in case the primary is lost. ***The envelope also contained the ATM pin and the Internet password for the prepaid card.***

This process reveals any gaps, which can either be exploited by an internal employee individually or in collusion with bad elements. Here is why:

1. A smart Bank executive can keep copies of passport and visa of a number of customers based on the balance in their account and the frequency of operations. Consider that most people get 10 year multiple entry US visas or H-1Bs so it will not be difficult for the Bank executive use this documentation after 3 or 6 months. A Bank executive can very well plan a fraud by using copies of the passport and visa and can easily fill the forex prepaid card request form and self approve the form along with the signature on it. So if the passport copy and visa are proxy for some kind of control (I think it's more compliance requirement than any kind of control) than that is not really going to work.

- Continued on Page no. 2

The Full Picture – continued from page no. 1

2. The ATM pin and Internet password are both contained in the envelope, which has the prepaid card. This is a big gap. Here the Bank should have used an out of band communication channel for the ATM and Internet pin. The Bank could have sent me the ATM pin on my mobile and asked me to set the Internet pin for the card by logging on to their website and use the ATM pin and answer a challenge question linked to my base account like the digits of my savings bank ATM card or a 2nd factor authentication like OTP.

3. But the best part was not this. Remember this was a chip card with EMV inscribed on it (and I had specifically asked for one and I believe Banks are now required to issue chip cards as per the new rules issued by the Central Bank of India - RBI). So when I used this card in Europe, I thought I will be asked to input the pin whenever I use this card (which I so religiously changed in India at the Bank's ATM). Not once when I used this card at a merchant establishment was I asked to input my pin. The merchant did not even check my signature (which is a different issue altogether). Just swiped the card and as soon as the receipt came out, asked me to sign it and I was on my way. So where was the basic protection this card was supposed to provide me in the 1st place. I might have as well been carrying cash in my pocket! It defeated the biggest selling point of the Prepaid travel card in India - that you are rid of the headache of carrying cash.

What the above experience highlights is the failure of the security controls in the process and therefore really no value add of the service to the customer. Not the Application functionality or the Technology. And therefore the need to look at security in a holistic sense i.e. the process, the people and the Technology. When I compare my experience of the security provided by travel card with that of carrying travelers' cheques, I find the security provided by the travelers' cheques is significantly higher. I, therefore, by no means am suggesting that we go backwards. We just need to review the prepaid cards process and make it as secure.

In the traditional sense technology risks or Information security risks have always been seen in a silo. Typically corporates have a process audit conducted by internal auditors, Than they have a different set of auditors who do the ISO 27001 audit (which is the IT process audit) and than a third auditor to do the Infrastructure and network audit and a fourth set of vendors like Net-Square to undertake Ethical hacking (what is often referred to as the application audit). While each of the auditors / vendors bring their own specific skills and expertise, it is important to put all this together and look at the full picture. Something I believe the information security department may not be able to do given the operational load that they carry. ***Recognizing this need, we at Net-Square are now offering a business process review service.*** In this we will look at one P&L process in its entirety and comment on whether the security architecture and process at every level matches the residual risk that the Organization is comfortable taking. We know that this requires us to bring to fore tremendous domain understanding of the business. For this we have created a framework that will help us understand the business dynamics and than evaluate the security architecture around a business process. In this process, we will also look at the Risk Management systems. We believe we are well positioned to do this due to the diverse experience brought by each one of us at Net-Square which ranges from quickly building a good understanding of business to deep technical knowledge of applications, devices and different technologies.

We all know that no security architecture is foolproof. The purpose is to make the job of the attacker / fraudster / mischief-maker very difficult. The architecture has to be like doors within doors. The idea is to frustrate the attacker. Creating disjointed sub-process within a operational business process can create cracks, which is exactly what smart attackers / fraudsters are looking for. I am sure our friends in the BFSI, Hospitality, Travel and Telecom sector will find this new service very interesting. We are looking for our first mandate in this direction.

- Hiren Shah, President, Net-Square Solutions Pvt. Ltd.

Educating customers on keeping their accounts safe when on holiday

It is summer in the northern hemisphere and many families will be off on a holiday. In the good old days it was said that one should not broadcast a vacation trip as that may alert a thief. There were many innovative gadgets designed to keep the thieves out. All that is now passé. The focus of the thieves now is not on the physical assets, but digital assets. This is not in any way to say that there is no danger of a break in!

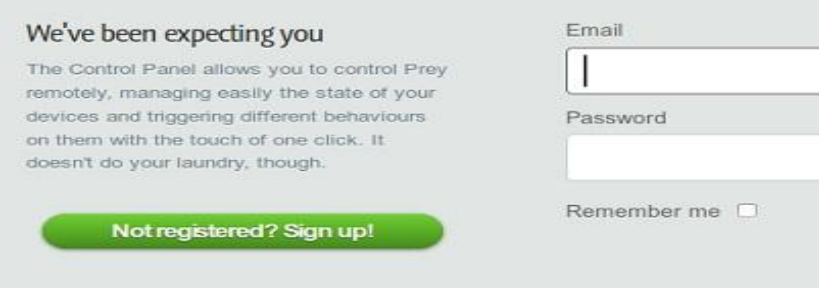
Whenever a customer of a Bank or a Financial Institution (FI) suffers a fraud eventually there is a –ve consequence of that on the Bank or FI as well. Either they have to cough up the loss or they end up losing the customers, both not desirable outcomes. We think it is therefore very important to educate the customers on specific steps they can take to keep their accounts secure especially while they are on vacation.

Here is a list of guidelines that they can ask their customers to follow, when they go on long vacation:

- Move all banking / financial transaction authorizing material like a check book etc. in a bank locker.
- Ensure that the data on their computing equipment like laptops, desktops etc. is encrypted.
- Move all external storage devices like external hard disks etc. in a bank locker.
- Enable mobile alert service if they are not already using one for all kinds of transactions including banking, credit card transactions etc.
- Ensure that the mobile number registered with the Bank / FI has roaming facility and can receive incoming SMS (normally that is free)
- And use only chip cards!

There are also steps that Banks and FIs can take. But that we will tell you in confidence. Happy Vacations!

Net-Square Team



Phishing!

Every attack vector has a life cycle. When it starts off the impact is the highest. And the growth of an attack vector most often points to the ease with which it can be carried out and the stealth with which it can be carried out. As time goes, more people become aware of it and it becomes more and more difficult to pull it off. But there are the rare few that live on for years.

One such attack vector is Phishing! It has been in existence now for more than a decade and despite a variety of products and user education efforts it still tends to raise havoc and there are many instances that come to light every year in the press.

One reason for this is that Internet penetration is growing in the smaller towns and cities of 3rd world countries that bring in new set of vulnerable users. But the success of Phishing is not just limited to the 3rd world countries; some very famous companies have been targets of recent phishing attacks. This list is available at www.fraudwatchinternational.com. In one such example, a phishing mail was sent out to customers asking for their online banking account verification details. The reason given for such a mail was of recent service interruption due to which customers needed to re-fill/update their details on the online banking portal. A similarly fashioned attack was earlier carried out on other Global Bank's customers, this time reason being specified as blockage of account due to many login attempts.

A recent report from Symantec has revealed that in India alone, the financial sector has lost more than Rs 1.3 Billion (US$ 25 Mlln) from phishing attacks over the past three years. In India, the IT industry bears the brunt of having been the target of the most number of phishing attacks with 14.4%, while the education sector ranked second with 11.9% of such attacks. This is not surprising since a very large number of young and technologically inclined users work or operate in this sector. In keeping with this trend, attackers have now started targeting phishing attacks to smart mobile devices. It doesn't help that an Android malware variant, which could send and receive commands (like launching applications on the phone), was found on about 1 million mobile phones. The malware can update its script to evade anti-malware detection.

Not only this, hackers are targeting gamers by spreading fake versions of popular games. These apps aggressively push ads and gather personal information from the infected mobile devices. The challenge for the individual is further complicated as it is very difficult to ignore the attractions of participating in the latest fads and the attackers knowing this come out with free versions of popular games and applications, which actually are infected with the malware.

So how can an organization play a role in it? Net-Square believes that adoption of BYOD could help solve this crisis. With the personal device now under corporate IT governance, many threats, which would have otherwise been difficult for the individual to detect can be detected by the policies and controls implemented as part of the BYOD rollout policy. Highlighting this advantage can help a CIO accelerate the penetration of BYOD rollout and result in tremendous cost savings to the Organization and at the same time provide enhanced security to the individual on the smartphone devices.

Considering the new threats on the mobile and the challenges of BYOD, we at Net-Square are always happy to offer our User awareness training program in which we show a few demos to bring home the point that this is a "Clear and Present Danger" and not some ghost that people raise from time to time.

- Hardik Kothari, Business Development, Net-Square

Tips for secure usage of Corporate social media accounts

Increased online presence does come with a risk. The past few months have witnessed Twitter accounts of large organizations being hacked. Recently in April, news organization Associated Press' Twitter account was hacked and they posted fake breaking news tweet. The problem that lies here is the speed with which such false news get spread amongst people. It just does not end here. There have been cases in the past where attackers have broken into a person's social networking account, accessed details of his confidential information and then moved on to conduct financial transactions!

So how do we protect official social media accounts like Twitter, Facebook, LinkedIn from being attacked? Net-Square believes that employee awareness is of paramount importance in ensuring security. Few points which can help are:

1) Avoid using corporate email addresses for such accounts. Corporate email ids make it easier for attackers to guess logins. A different id will make it harder for assumption.

2) Use strong passwords for logins. Still better, consider password management solutions which help share passwords between teams without actually making them visible.

3) Implement software available to manage social media accounts on a single platform. For eg: A software Hootsuite helps to manage social media like Twitter, LinkedIn, Facebook, MySpace, Mixi and many more on a single platform. This software also allows employees to tweet without having to know the company password for the account.

- Net-Square Team