August 2012

V e c t o r

A Net-Square Initiative

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

Saumil Shah
CEO, Net-Square
reach him at saumil@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 is the training programs. Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~Breaking~~ Hacking News:

Two-Factor authentication for cloud storage company, Dropbox, after security breach

In the first week of August, Dropbox revealed that it had been hacked yet again! Some of the user accounts were hacked, but an employee account was breached. Interestingly, the said employee's account had a project file that contained "user email addresses"! A valuable find for hackers, they can now target users easily. To counter this, Dropbox is implementing two-factor authentication, which will require users to give two proofs of identity.

To read more visit article 2240161007: searchsecurity.techtarget.in/news

From 0 to Fix

One of the ongoing jokes in the information security industry is that "every day is a 0-day". New bugs are being discovered daily. The recent Java 7 exploit (CVE-2012-4681) found in the wild has captured everyone's attention. This bug has the potential to cause widespread damage. As I write this, almost after a week of its discovery, organizations and individuals are still being targeted by this exploit. Governments, intelligence agencies, underground outfits and script kiddies are having a field day "owning" your systems. The logical question that follows is "so, how do I prevent myself from being owned?" Vendors have always pursued the noble goal of creating bug-free software. What many vendors miss is the "TIME TO FIX" factor. Time-to-fix is the time taken from the bug's first discovery to a patch or update made available to the customer. If you are building software or responsible for the security of your organization's applications, ask yourself the following questions: "How fast is my bug fixing process?","What is the average turn-around time of all bugs fixed in 2012?", "What has been my fastest time-to-fix? My slowest?" Scoring guide: Less than 48hrs - Excellent. 48-72hrs - Fair. More than 72hrs...I will leave you to work out the uneasy answer, since I don't want to be impolite.

Chris Evans, who heads the Google Chrome security program has set an aggressive time-to-fix goal of less than 24 hours. And his team has come good on this promise. The Pwnium contest at CanSecWest 2012 in March saw two Chrome bugs fixed and turned around in less than 24 hours. Users worldwide had a Chrome patch before the conference was over. Google paid USD 120,000 in bug bounties as an appreciation for the bugs turned in. Pwnium 2 shall be held at Hack in the Box, Kuala Lumpur in October (where yours truly is speaking as well as training). I am told that Google is bringing a treasure chest of 2 million dollars to be paid out in bug bounties. This is solid security!

I must also mention the herculean efforts made by Microsoft. "Patch Tuesday" is an important monthly event for IT professionals worldwide. Microsoft releases patches for its entire product line on the second Tuesday of every calendar month. Sometimes there is an extraordinary Patch Tuesday in the same month to address critical fixes. Although a bi-weekly update seems slow in light of my personal 72 hour benchmark, it is a mammoth task to ensure stability of a bug fix across a vast and diverse product line as Microsoft's. Vendors of other high exposure software are not as mature as Microsoft or Google. Adobe, Apple and Oracle are learning this lesson the hard way. They have been struggling with bringing in a strict time-to-fix regimen.

Speed of bug fixing is something every organization should pay serious attention to. We have found this to be the Achilles' heel for many of our clients. They struggle to remediate their vulnerabilities simply because their outsourced software vendors don't have their act together and take months to fix them. In the past we have helped our clients on remediation through our training programs. This week we are piloting a novel approach to help solve our clients' problem through an onsite service. A Net-Square analyst will work onsite with the internal development team or the software vendor to ensure the vulnerabilities are fixed. This they will do sitting next to them, helping them understand what the issue is and helping them literally code appropriately for it.

Incidentally, until Java 7's latest bug, CVE-2012-4681, is fixed, I personally have uninstalled Java browser plug-ins from all my systems. I probably intend to keep it this way too.-- *Saumil Shah, CEO, Net-Square*

Two-Factor Authentication: Enough for your Application and User Security?

2FA or Two Factor Authentication as the name suggests, relates to a form of approval which requires a user to present two or more of the 3 authentication factors. These are: "something the user knows (eg. Password, PIN)", "something the user has (eg. ATM card, Smart Card)" and "something the user is (eg. Biometric characteristic such as fingerprint)". Not a new concept for the masses in this era of netbanking and internet trading. 2FA has become increasingly important for online applications because of the ever increasing hacking attacks. Recently, a US based company offering free cloud storage services was hacked where few accounts were broken into and one employee account containing user data files was breached! This sounds dangerous as hackers may get confidential data from account owners, since this service was being used worldwide where companies were storing important data online. This Company then decided to implement 2FA to prevent such attacks.

So be it social networking websites, business mails, or online banking transactions, taking cue from all such attacks, the regulatory bodies world over have drafted several guidelines which banking and financial organizations have to adhere to in their countries. In India, Reserve Bank of India, has issued a guideline mandating all banks in India to have a mechanism which ensures 2FA for all online transactions carried out by the bank users. In 2010, RBI also mandated 2FA for transactions happening through IVR Channel. Even the Capital Market watchdog in India, SEBI, has mandated usage of 2FA mechanism by all the broking members. Such is the result of RBI directive, that banks have rushed with tenders to implement 2FA.

While having 2FA in place is a good security measure, it is not the proverbial "silver bullet"! Even if 2FA is in place, users use same credentials for multiple logins and transactions, which makes it easy for attackers to gain information about the user through a host of other ways. Like for instance the Man-in-the-middle or Man-in-the browser attacks.

A recent security incident where the hactivistgroup UGNazi were able to hijack CloudFlare CEO Matthew Prince's account amply highlights this. Even though Prince was using Google's Two-Factor Authentication, what enabled the hackers to gain access to Prince's Gmail account were other weakness in Gmail and the telephone provider AT&T's systems.

When I recently spoke with the CISO of a large public sector bank, he said that while they are implementing 2FA, he doesn't believe 2FA is going to be enough. They planned to continue to conduct periodic application security tests and follow secure coding practices. This is important because applications undergo continuous changes and this makes them vulnerable.

In a separate dialogue with another CISO it was revealed that what is troubling him currently is the ease with which fraudsters are able to get their hands on duplicate SIM cards rendering the 2FA in the form of mobile pin completely useless.

Two-Factor Authentication has never been enough because sophisticated fraud simply leverages the authentication process. A right approach is to have a 3 level check: Periodic security checks of the application itself, Social Engineering exercise, and lastly the two-factor authentication implemented.

-Hardik Kothari, Business Development, Net-Square Solutions

Net-Square at the Hack-In-The-Box, Kuala Lumpur Conference!

Celebrating a decade of HITB Security Conferences, Hack in the Box is back! This time with "Ten Years in the Box" - 10th Anniversary Conference marked with a line-up of over 42 of some of the most popular speakers from the past ten years. And yes, Net-Square will be there! Saumil Shah, CEO, Net-Square will speak on "Innovative Approaches to Exploit Delivery" and conduct a training class "The Exploit Laboratory 7.0" at the event. So hurry and grab your seats now! To register online visit:

- **Saumil Shah: Innovative Approaches to Exploit Delivery** http://conference.hitb.org/hitbsecconf2012kul/saumil-shah/
- **Training: The Exploit Laboratory 7.0** http://conference.hitb.org/hitbsecconf2012kul/tech-training-8-exploit-lab-7/
- **Conference Details:** October 8-11, Hack in the Box: Kuala Lumpur.

Project Hellfire: Records stolen from hundreds of websites

A massive leak of data, allegedly more than a million records, has been stolen by Hacking group, "Team GhostShell". They along with two other associate groups compromised hundreds of websites, calling it Project Hellfire. This has affected a wide range of verticals from financial, to law enforcement as also family owned businesses. Data which was compromised consists of email ids, phone numbers, home or business addresses, immigration status and more. According to SecurityWeek, a US based IT Security Forum, which examined the data, the leak is less sensitive in some cases and useless in a lot more cases. To read more visit: *http://www.securityweek.com/project-hellfire-millions-records-taken-hundreds-sites*