April 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~~ Hacking News:
UK banks hit by Ramnit banking malware!
According to a May1, 2013 article in online portal thehackernews.com, a dangerous variant of Ramnit worm has been discovered targeting UK's banking sector. The malware reportedly avoids detection by going into an idle sleep mode until its intended victim logs into their online bank account. Once logged in, it activates and presents them with fraudulent phishing message. While victim is reading messages, Ramnit connects to its control server and sets up wire transfer! To read more visit url: http://thehackernews.com/2013/05/uk-banks-hit-by-ramnit-banking-malware.html

Sometimes it's about the functionality also….

Over the years our focus at Net-Square has been to find holes in the application's code. Holes left by developers due to shall we say lack of awareness of how to code securely. But we are now finding that this is not the only reason that Enterprise applications could be vulnerable to a fraud or data breach. It is just plain design of the functionality in the application. Let me give you couple of examples.

Suppose you are building a procurement management system. How would you implement Authorization module? You will find that in most systems there will be a System Administrator role defined that grants rights to different menu items in an application to other users. Or in more mature applications the System Administrator grants roles to users. And Roles are mapped to different menu items available in the system. Very often we have found that the way the functionality has been set-up, the System Administrator also creates new ids or updates master data of users (like mobile numbers in case of 2-factor authentication). In such a scenario, how difficult is it going to be for a System Administrator to create a dummy id and give the necessary rights to oneself to commit a fraud?

Take another instance. Applications are now becoming more complex and need to collaborate in real time with other applications across the world. This is often done through implementation of technologies like web services or ESB. We have come across applications where if the data between two systems goes out of sync because of a link or hardware failure, the data is brought in sync manually and there is support id created to do that. We are quite amazed to hear in some of our interactions when we ask the question "So who has access to this support id?". Back pops the answer "I, xyz and abc. That way if one of us is not available the other can correct the data and the process can move forward." What if the person doing it alters the data and you are talking about applications supporting commercial transactions involving thousands of dollars. Whenever we have raised this question, we have got perplexed looks. Something like, someone will notice something is not right, I guess.

With increasing number of such instances, we have now added another value added service as part of our Application Security offering. We now offer functional security audit of the applications either as part of our normal VAPT exercise or as a separate engagement. In this exercise we review the business objective of the system, establish the information security requirements and assess if the functionality of the system adheres to the information security requirements or there are any inherent weakness in the way the business process is functionally translated into the system. As part of the functional security audit, we interview the Business managers whose business is supported by a given application and we interview the IT Application owners who support the application. The purpose of the interview is to gauge the acceptable level of security from the business team and the seriousness of the IT team in implementing the right checks.

There are some very good behavioral stereotypes we have seen emerge from our interaction. One, business managers do not like the limitations introduced by information security requirements though they also do not want to lose information or competitive advantage due to loss of data or face any fraud situations. Two, the IT team is always stressed in trying to balance the business requirements with infosec concerns. And in doing so, sometimes, knowingly take risks. And they are not apologetic about it.

We at Net-Square know that one has to find the practical balance. Therefore we always advise the customers at the end of every such exercise on how to balance the business requirement with that of infosec. After all, we know how attackers behave so we know how best you should protect your business. And through our experience, we can also tell you, there is no silver bullet. To know the value of conducting such a review, call us. You will be surprised!

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

Using 3rd Party Apps? Make sure they are secure!

Business today cannot ignore varied creative spaces for marketing their offerings. And this is exactly the reason for a tremendous rise in 3rd party applications, be it standalone programs or small plugins that add functionality. Parting with the earlier trend where companies used to depend heavily upon enterprise software providers and a few others for all their applications, people now want to have a go at everything, which seems more convenient and helps them network. Employees can't seem to live without social networking applications like Facebook, LinkedIn, Twitter, MySpace and various other applications offered by 3rd party providers making them essential for today's business.

According to a mobile market research and consultancy firm, research2guidance, the market for app development services, including application creation, management, distribution and extension services, will grow in value to US $100 billion in 2015. Although these applications and social networks are primarily intended for consumer use, companies are increasingly recognizing their business benefits. This creates a unique challenge for the IT department. In addition to the benefits, they can negatively impact productivity, network bandwidth, users' privacy, data security and the integrity of IT systems (via malware and application vulnerabilities). A lot of these applications come with severe vulnerabilities and exposing business and personal data to them poses a high security risk. Previously, only malware was a major threat. But today, about 75% of cyber attacks happen due to vulnerabilities in third-party applications.

General perception amongst companies is that by investing in patch management, and by patching third party applications, they will be safe. But there is more to it than just patch management. Net-Square, during its network and application audits has observed that such patching devices, even if implemented and configured, fail to ensure 100% patch management. Also enterprises are always at the mercy of third-party vendors for patching the flaws and preventing a software exploit. In some cases, the patches are released months after a flaw has been detected. And in the meantime new flaws emerge. In order to be secure, 3rd party applications should be managed more proactively. Some do's and don'ts that Net-Square recommends are:

- Depending upon risk, companies should define and offer selective usage of these applications.
- Frequent security audits of all 3rd Party applications should be implemented. A good practice would be to incorporate a mandatory requirement of security audit certificate in application procurement tender. This would enforce software product companies to implement secure coding practices and get audited from an independent security firm.
- Only implementing an automated patch management system will not help the cause. There has to be a team of knowledgeable people managing this system and ensuring patch adherence.
- It is advisable to implement two-factor authentication for 3rd party applications. Two-factor authentication that uses out-of-band authentication such as a PIN sent to a smart phone, does require a hacker to go to extensive lengths to beat it, and so adds an additional layer of protection.
- Conduct security awareness trainings for business users, application IT teams and Infosec teams at regular intervals to educate and sensitize teams on ongoing attack trends and how they can prevent them.
- Finally, even employees can ensure secure and safe usage by practicing a few things like using different passwords for their personal and business accounts and regularly changing them. Define privacy settings in all social media applications such that personal information is not exposed. Immediately revoke access to third party applications if employees sense anything fishy in their accounts. These are small steps, but can go a long in ensuring safe and secure usage!

-Hardik Kothari, Business Development, Net-Square Solutions

Tips to use public wifi hotspots

The next time you are in a mall and want to access your mails via wifi, think twice. You may not be very lucky with attackers finding a way to your confidential information through the public wifi. Spare a thought when you hit a public open wifi next time you are in a mall or any kind of public place. Do you know who has put it there?

According to researchers, public wifi usage has gone up 240% in the past year. Part of this rapid increase in the use of such public wifi is due to the growing use of smart phones and tablets. While it is advantageous as it provides convenience to people and Internet on the move, but it is also easy for attackers to target users of such open wifi hotspots who transmit any traffic which is not encrypted. Attackers can sniff unencrypted traffic and view sensitive data in emails or http headers or even user id and password, if the session with the server is not encrypted. There are numerous tools available to an attacker to hijack sessions and automate monitoring and analyzing of traffic. What if you are accessing your bank account?

Now with BOYD coming into vogue in many Organizations, the risk for Enterprise users of such wifi hotspots has also come into focus.

The solution to this menace cannot be observing certain rules when using wifi hotspots. That is just too much to expect of people. The solutions will have to be technology driven like:

1) Use VPN connectivity for accessing corporate data. A VPN will encrypt information traveling between user's computer and the company's remote network.

2) By default only connect to public email servers like Google or Hotmail using https. Make sure the same settings are reflected in the local email clients on all your devices.

Security on end user devices now has to be configured with the assumption that any Internet connectivity that the device connects on is compromised. Once you start with that premise, all security configurations will most likely be stronger. Stay safe!

- Team Net-Square