Yui Kee Computing Ltd.

Newsletter

November 2008

Contents

Pacnet Refuses to Discuss its Censorship

<web-link for this article>

Allan Dyer

To permit Pacnet a full and fair right to reply to my denouncement of their censorious Terms and Conditions, I emailed and called Pacnet, drawing their attention to the article and asking for their response. In a letter dated 05 November 2008, Pacnet responded:

Regarding your conversation with our Customer Service Officer Elaine Wong, we reiterate the points raised in our Mr. Johnny Cheung's letter dated 28 July 2008 (copy attached).

The email referred to says, as reported in the previous article, "*Your comments on our T&C are well received and noted. Please kindly understand that the T&C is structured to strike a fair balance among the law, the customer's benefits as well as Pacnet's benefits.*"

It is clear that Pacnet is unwilling to discuss the powers of censorship their updated Terms and Conditions grab. They have made no justification for their stance, nor offered any counter-arguments to the criticisms I raised.

Pacnet have not even responded to my claim that my denouncement is in violation of their updated Terms and Conditions, and, therefore, if Pacnet think they apply, they should censor the article. Pacnet may be practising an insidious form of censorship: quietly intimidating those who can be easily frightened. Who has control over Pacnet's decisions?

In order to preserve the free flow of information and safeguard the freedom of expression enjoyed by Hong Kong people in the context of the internet, we need to ensure that ISPs in Hong Kong do not make arbitrary decisions about what content is acceptable or permitted. We have laws on public decency, copyright, and computer crime, and authorities to enforce those laws. ISPs should provide open communication for all legal content. We must ensure ISPs do not usurp the power of our courts and are not allowed to control what we see and say, whether that is for their commercial interests or hidden political purposes.

More Information

Why Should the Government Curtail Free Speech When ISPs Will Do It?
Yui Kee Warns: CPCNet Puts Customers At Risk; OFTA Adopts a "Hands Off" Position

How can children be protected from obscene material online?

F-Secure has Head in Cloud

<web-link for this article>

The Internet security industry needs the speed and power provided by cloud computing to be able to respond to the exponentially growing volume of cybercrime. In a recent press release, F-Secure commits itself to developing cloud computing and reputation-based services - harnessing the power of end-user systems and collaborative intelligence in the network to fight cybercrime. This creates a strong, trusted connection between the security provider and the end user, allowing, F-Secure claims, unprecedented quality and speed of protection for its customers.

F-Secure launched its real-time protection network in September 2008. It is an implementation of the in-the-cloud reputation service, capable of supporting several types of security solutions. F-Secure DeepGuard 2.0, which combines local analysis of program behaviour with the use of a real-time protection network for identifying both good and bad software, scored an industry first in the same month with its instant reaction times and global protection against new threats. This is important in today's dramatically changed threat situation where the Internet is facing a deluge of new malware and variants that make traditional heuristics or signature-based solutions just too inefficient and slow.

Pirkka Palomäki, Chief Technology Officer at F-Secure, said, "Our real-time protection network is based on in-the-cloud computing. It has been designed to support a wider range of security services than just antivirus and F-Secure is now further enhancing many of its services to use the power of cloud computing".

Palomäki continued, "Looking towards the future, F-Secure's real-time protection network has the architecture and potential for checking the reputation of any objects, such as applications, sites, documents or even phone numbers. It provides more nuanced information, for example whether an application is 'productive' or 'violent'."

F-Secure says that this progression into cloud computing is natural for the company and considers it critical for addressing future threats. F-Secure has been building in-the-cloud protection for years. Its first form was been the creation and maintenance of Network Operation Centres globally since 2001, which laid the groundwork for the real-time protection network. Actual in-the-cloud protection has been implemented since 2006 with F-Secure's antiphishing services that use network-based verification of threats.

T. Sean Obrey, F-Secure's Head of ISP Business, says, "We have over 170 partners globally and network operation centres on all continents. These global networking services and solutions have been developed to support our business. It is very natural step for us to now provide our protection services, via our Service Provider partners, to their end customers using the cloud experience that we continue to develop."

The F-Secure real-time protection network is currently being used by F-Secure DeepGuard 2.0 which is included in the F-Secure Internet Security 2009 and F-Secure Anti-Virus 2009 consumer security products, as well as the corporate F-Secure Client Security 8 solution and others being launched this year.

More Information

F-Secure Leads Internet Security Industry in Developing ‘In-The-Cloud’ Technology

Hong Kong Clean PC Day 2008

<web-link for this article>

"Hong Kong Clean PC Day 2008" is 20th November 2008. The day is organised by Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), the Office of the Government Chief Information Officer (OGCIO) and Hong Kong Police Force (HKPF) and is intended to promote awareness about information security among PC users.

There will be a free seminar, in Cantonese, covering topics including botnets, threats in the Web 2.0 era, Foxy and data leaks, risks of surfing in public spaces, different defences, and a panel session.

Title	Hong Kong Clean PC Day 2008 - Public Seminar
Date & Time	November 20, 2008 (9:00am - 5:30pm)
Venue	Lecture Theatre, Hong Kong Central Library, 66 Causeway Road, Causeway Bay, Hong Kong
Language	Cantonese (with English terminology)
Fee	Free
Organisers	HKCERT OGCIO Hong Kong Police Force
Enquiry	Tel: 2788 5884

More Information

HKCERT Upcoming Events

LoveLetter Worm Inspires Romantic Comedy Movie

<web-link for this article>

Director Francis de la Torre is working on "Subject: I Love You", a movie based, in part, on VBS/LoveLet-A, the email worm that spread around the world with unprecedented speed in May 2000. Set in Manila, the Philippines, the story revolves around a romance between an American girl (played by Briana Evigan) and a Filipino boy. She leaves the country, and he writes an email worm in a misguided attempt to contact her.

Slightly cuddly senior technology consultant and aspiring movie-star Graham Clueley expressed concern that the movie might make virus-writing appear cool or even sexy.

VBS/LoveLet-A caused data loss by overwriting JPEG files and attracted considerable media attention by its speed of spread. Manila native Onel de Guzman was reported to be the author, but he was never tried because the Philippines had no applicable laws at the time. There was no suggestion that a romance had inspired the worm.

More Information

A virus romantic comedy?
Love bug worm inspires Asian film
Subject: I Love You (2009)
'Love Bug' Computer Virus Inspires Quirky Romantic Comedy 'Subject: I Love You'
Sophos: VBS/LoveLet-A

SSH Security Advisory: Plaintext Recovery Possible

<web-link for this article>

A design flaw in the SSH protocol has been discovered by Martin Albrecht, Kenny Paterson and Gaven Watson from the Information Security Group at Royal Holloway College, University of London. The design flaw allows an attacker that is able to listen to an encrypted Secure Shell (SSH) connection and actively steal the network connection (TCP) to, in some situations obtain up to 4 bytes of cleartext data from the session. The attack attempt causes the attacked connection to be disconnected immediately. The attack works only against protocol sessions that are encrypted using a block cipher algorithm in the cipher-block chaining (CBC) mode. Exploiting this vulnerability is very difficult.

As the issue is caused by a protocol design flaw, it is believed to affect all SSH implementations. It has been confirmed as affecting:

- OpenSSH 4.7p1
- SSH Tectia Client and Server and ConnectSecure 6.0.4 and older in the 6.x series
- SSH Tectia Client and Server and Connector 5.3.8 and older in the 5.3.x series
- SSH Tectia Client and Server and Connector 5.2.4 and older in the 5.x series
- SSH Tectia Client and Server and Connector 4.4.11 and older in the 4.x series
- SSH Tectia Server for Linux on IBM System z 6.0.4
- SSH Tectia Server for IBM z/OS 6.0.1 and 6.0.0
- SSH Tectia Server for IBM z/OS 5.5.1 and older
- SSH Tectia Client 4.3.3-J (Japanese) and older in the 4.x-J series
- SSH Tectia Client 4.3.10-K (Korean) and older in the 4.x-K series

SSH Communications Security has issued a security advisory concerning this vulnerability for its SSH Tectia product-line and has released fixed versions of the affected products. Currently active Maintenance Customers can download the installation packages from SSH Customer Download Centre at https://downloads.ssh.com. The products provided there include valid license files.

In the absence of a fixed version, the most straightforward solution is to use CTR mode instead of CBC mode, since this renders SSH resistant to the attack. In practice this is achievable with the SSH Tectia products by utilising either CryptiCore or Arcfour encryption algorithms.

The attach is considered very difficult, it recovers only four bytes of cleartext, and the connection is broken by the attack, so the chance of this vulnerability being used to achieve a significant security breach in most situations is small. However, SSH users will be naturally cuatious, and therefore want to apply the fix without delay.

More Information

CNPI InfoSec vulnerability disclosure ID: 3716 Vulnerability in SSH
Plaintext Recovery Attack Against SSH
CPNI Vulnerability Advisory SSH Plaintext Recovery Attack Against SSH

Paypal Language Features Inconvenience Users

<web-link for this article>

A botched roll-out of a new Hong Kong Paypal website left some customers unable to access their accounts. The problem affected visitors to the new Hong Kong Paypal site: www.paypal.com.hk, and the international site: www.paypal.com, presenting a webpage in

Chinese, without readable links for other languages. It seems that Paypal ignores the W3C recommendations on language negotiation, and has not learnt from the failures of Trend Micro and McAfee Associates.

Paypal announced their new website in an email to Hong Kong-registered customers, boldly claiming, "PayPal now speaks your language! Find what you need in Traditional Chinese or English". Oddly, the message included English and Chinese text, but the MIME content-type header was "text/plain;charset=iso-8859-1", a character set that does not support Chinese. Visiting the .hk site presented an entirely Chinese page (screenshot below), with no obvious option to change the language. OK, you might think, no problem, go to the international site and check - but Paypal also configured their international site with a Chinese-only page for Hong Kong customers (screenshot below).

Paypal's new HK website

Paypal's Hong Kong customer service were able to help - it is simply necessary to clear the browser cookies in order to get the English version of the site. However, contacting customer service is more of a problem... customers can, of course, login and check the contact details page, but what sensible customer would enter their username and password, and start exploring links in a language they do not understand, on a site that handles their money? One method is to check the whois record at HKDNR for paypal.com.hk - this provides the company name, eBay International HK Ltd., but no phone number. Directory enquiries cannot provide a phone number for the company (eBay was unable to explain why their phone number is not listed). However, calling HKDNR provides the direct line of the eBay Administrative Officer, Amy, who was able to provide customer support numbers for Paypal (35508574) and eBay (35508586) in Hong Kong.

Paypal's international site, seen from HK

Although the workaround is simple, questions remain for the company:

- Why isn't Paypal referencing the W3C standards and recommendations: using the

  Accept-Language HTTP header and

providing a usable language-change feature?

- What was stored in the Paypal cookie, and why?
- How will the company improve its contact methods so that customers without website access can contact them easily?

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/