Yui Kee Computing Ltd.

Newsletter

July 2008

Contents

Pwnie Awards for Security ... and Security Failures

<web-link for this article>

You've heard of the Oscars, Palm Doors, 香港電影金像獎, Pulitzers, and Rory Awards. Every field of human endeavour needs to acknowledge its successes and failures - even terminal stupidity (the Darwin Awards). Since 2007, the Information Security field has had the Pwnie Awards and this years nominees for the second annual award have been announced.

The nine award categories include the Best Server and Client Side Bugs, Mass 0wnage, Most Innovative Research, and Most Epic Fail. The Best Song category probably has the greatest entertainment value, with clever lyrics, although there is an advertising component - especially for Kaspersky's "Packin' The K!" rap.

For the Lamest Vendor Response, Linus Torvalds has been categorised as a vendor for his kernel non-disclosure policy rant, though that seems to pale into insignificance compared to McAfee's refusal to categorise XSS as a vulnerability for their "Hacker Safe" certification program, or NXP's threat to sue Radboud University Nijmegen over a paper on fundamental flaws in Mifare Classic, the contactless smartcard used (as Oyster cards) on London's transport system.

The awards ceremony will be held at the BlackHat USA reception, Caesar's Palace, Las Vegas on August 6th.

More Information

Pwnie Award Nominees
Pwnie Awards 2008
Pwnie Awards celebrate best and worst of security
Pwnie Award Winners 2007

Why is Website Language Negotiation So Poorly Adopted?

<web-link for this article>

Allan Dyer

The Accept-Language HTTP header has been part of the web standards for over a decade, but still many multi-lingual sites ignore it and, in the worst cases, use unsuitable methods for selecting the language. An example I came across recently is the latest version of the Trend Micro website.

The basic idea is that the user's browser sets a header in each request, specifying the user's language preferences, and the website responds with the most appropriate version of the document that it has available. The user can set their preferences in their browser options (in Firefox, Tools -> Options -> Advanced -> Languages, Choose), and the browser will take care of sending this to every site they visit.

What happened on the Trend Micro site? Until recently, going to www.antivirus.com got you Trend Micro's English site. On a recent visit, I found that I now got a Simplified Chinese version of the site. In fact, there is a permanent redirect on http:/www.antivirus.com/ that points to http://www.trendmicro.com/, and that site serves a permanent redirect to http://cn.trendmicro.com/cn/home/. It appears that, in their wisdom, Trend Micro has decided to use the location of the IP address to determine the language the user requires. They have also decided that Simplified Chinese is the most appropriate language variant for Hong Kong. Wake up, Trend! Traditional Chinese is the most commonly used form of Chinese in Hong Kong.

In Trend Micro's world, countries have a single official language (Hong Kong has two official languages), and no-one visits or lives in another country. What about expatriates, tourists and business travelers? Trend does offer a way out - the first line of the site says, "This site is for visitors in China | United Kingdom | 全球网站", the last two being links to alternate sites. Of course, unless you understand Chinese, you will not realise that the Chinese text says "Worldwide".

So, the English-reading visitor, overcoming their annoyance, can follow the link to the UK site. where the top line reads, "This site is for visitors in United Kingdom/Ireland | Worldwide". Following the Worldwide link, and clicking Asia on the map reveals that the recommended URL for Hong Kong (and most other places in Asia) is http://apac.trendmicro.com. That site is in English.

No doubt Trend Micro considered making their website multi-lingual an improvement, but they spectacularly failed to consider minority visitors. If I was planning the site, I would first consider that they provide two types of information: information that is location specific, such as support contact points and local distributors, and information that is global, such as virus descriptions and product features. The global information should, ideally, be available in all languages, regardless of location. The location specific information might be restricted to particular locations, and to the official languages (note the plural) for the location, if resources are an issue.

Of course, the Accept-Language header is not always correct - the user may not know how to change it, and travelers in Internet Cafes will be a common example of users browsing from a machine that is not their own. The obvious way to deal with this is for sites to, by default, follow the browser language preferences, but to always provide links to the alternative language versions available for the current page.

Excellent discussion of the issues and configuration examples are available from W3C. To check your browser language preferences, try our Browser Language Preference Report.

22nd July 2008

Trend Micro is not the only anti-virus company that is confused about the relationship between people, countries and languages. The following message was displayed during the installation of McAfee VirusScan USB:

Select your country McAfee will use this information to determine which Web site can best serve you.

The list included, "Chinese - China", "English - Canada", "English - US". Is the user selecting a language, or a location? Is the Chinese Traditional or Simplified? Have the dialects in Canada and USA diverged so far that they should be considered distinct languages, or does the large physical separation of the countries make web-surfing slow between them? Which option, for example, should a Czech who learnt English in South Africa living in Hong Kong choose?

More Information

W3C Internationalisation FAQ: Setting language preferences in a browser
Browser Language Preference Report
W3C Internationalisation FAQ: When to use language negotiation
W3C Internationalisation FAQ: Accept-Language used for locale setting

Privacy Commissioner Recommends Improvements at the Hospital Authority

<web-link for this article>

Mr. Roderick B. Woo, J.P., Hong Kong's Privacy Commissioner for Personal Data, has made 37 recommendations for improving the protection of personal data to the Hospital Authority after his team inspected the Authority's systems following widely-publicised leaks revealed in April and May 2008.

The main recommendations will come as no surprise to information security practitioners, and include not using the Hong Kong ID card number as an identifier, or encrypting it, limiting the period of data storage, monitoring staff access, and regulating the use of portable storage devices. More importantly, Mr. Woo acknowledged the Authority's purpose, saying "The primary duty of the hospitals is to save lives. What we have done is to list out practical recommendations for the hospitals with regard to our concern for personal data privacy". He also recommended consolidation of the present multiple policies, "We find confusion caused by a profusion [of security policies]".

This is a busy time for the Commissioner, just last month he was making recommendations to the Immigration Department.

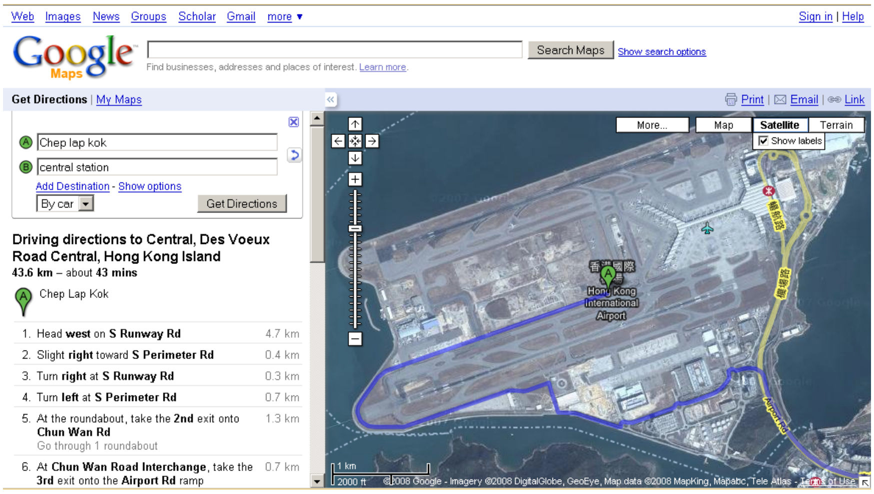
More Information

New data safeguards urged for hospitals
Immigration Department Learns Information Security Management Basics
Data Leak Disease
Privacy report: HK Hospital Authority must raise staff's data privacy awareness

Google Maps: Beware of Aircraft Noise

<web-link for this article>

Google Maps Hong Kong has recently introduced a "Get Directions" feature, however, it may need some fine-tuning as it appears to include roads that are not open to the public. For example, a trip from Chep Lap Kok starts with directions to drive down one side of the Airport south runway, and up the other side, rather than landside of the main terminal building. This should only be attempted while holding a security pass, in a vehicle with a flashing light on top, with due care and attention to Jumbos and Airbuses crossing your path.



Ⓐ Chep lap kok
Ⓑ central station

Driving directions to Central, Des Voeux Road Central, Hong Kong Island
43.6 km – about **43 mins**

Chep Lap Kok

1. Head **west** on **S Runway Rd** 4.7 km
2. Slight **right** toward **S Perimeter Rd** 0.4 km
3. Turn **right** at **S Runway Rd** 0.3 km
4. Turn **left** at **S Perimeter Rd** 0.7 km
5. At the roundabout, take the **2nd** exit onto **Chun Wan Rd** 1.3 km
   Go through 1 roundabout
6. At **Chun Wan Road Interchange**, take the **3rd** exit onto the **Airport Rd** ramp 0.7 km

First Sentence in the Edison Chen Sex Scandal Case

<web-link for this article>

The publication of private photos of female stars in sex acts with entertainer Edison Chen Koon-hei in January and February really put data privacy on the agenda for 2008. Three men were charged with offences relating to the incident, and now the first has been sentenced. Kwok Chun-wai, a 24 year old logistics clerk, pleaded guilty to three counts of publishing obscene articles between January 29 and February 6 this year, and was sentenced to two months in jail, suspended for two years.

Mr. Kwok had downloaded 140 celebrity sex pictures from the internet and saved them to a server. He then posted 25 hyperlinks on a Hong Kong-based adult discussion forum. This is selective prosecution, the photos do show explicit sex acts, and the act of storing them on a public server and linking to them is "publication", just as this newsletter is published on a website, but this type of material is not uncommon in adult internet forums. Kwok's lawyer complained that he had been made a scapegoat and it was unfair that other people who had posted the images online had not been prosecuted.

It is fortunate that the judge in the case had some sense of perspective. Kowloon City Court Principal Magistrate Andrew Ma Hon-cheung said that he was lenient on Mr. Kwok because he committed the offence out of "curiosity" and did not intend to cause harm to the celebrities.

The Edison Chen photos case does feature a serious crime: the unauthorised copying of private data from Chen's computer. Computer technician Sze Ho-chun is accused of that, and he will be facing three counts of dishonest computer access in October.

Data privacy has remained in the news this year because of repeated revelations of leaks from Government departments and major businesses, including the Hospital Authority, Immigration Department, Police and HSBC.

More Information

Edison sex pics publisher spared jail
Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal
Data Leak Disease

Sophos to acquire Utimaco

<web-link for this article>

Sophos, the anti-virus company based in Abindgdon, near Oxford, UK, has announced its intention to launch a voluntary public takeover offer of €217 million in cash for Utimaco, the encryption company based in Oberursel, near Frankfurt, Germany. In their history, both companies have grown their product offerings from technology fixes to full-featured solutions with management tools to meet the needs of businesses. Nowadays, Sophos's network access control, endpoint, web and email solutions simplify security to provide integrated defences against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. Similarly, Utimaco's range of data security solutions provide full 360 degree data protection for data at rest, data in motion and data in use.

This is not Sophos' first takeover, the company previously bought ActiveState and successfully integrated their advanced anti-spam solution, Puremessage, into their product line. It is also not the first acquisition of an encryption company by an anti-virus company: in 1997 Network Associates (formerly, and later, called McAfee Associates) bought PGP Inc. That combination was not successful, and the PGP assets were sold to PGP Corp., formed by former Network Associates employees, in 2002.

The offer is expected to be completed in October, as, in accordance with German takeover rules, Sophos has to publish a statutory announcement of a voluntary public takeover offer and issue the offer document describing the details of the offer to Utimaco's shareholders, following approval by the German regulator Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

More Information

Sophos to launch €217 million offer for shares in Utimaco Safeware AG

ISPs Slow to Patch Kaminsky DNS Vulnerability

<web-link for this article>

It is probably quite difficult for anyone technical not to have noticed the recent news about the DNS cache poisoning vulnerability found by Dan Kaminsky. Suffice to say that this is a vulnerability in the server software and it is the administrators of the servers that need to fix it as soon as possible. For most users, this means their ISP has to fix it, and many have not.

How serious a problem is this for users, and how can they protect themselves? It is very serious for users, because an attacker can use the flaw to redirect them to another site - potentially very expensive, if the site in question is for online banking! Discovering whether the DNS you are using is vulnerable is as easy as going to Dan Kaminisky's blog and clicking on the button "Check My DNS". If that reports a problem, contact your ISP or system administrator and ask them to fix it. While you are waiting for the fix, you can:

Change your computer's configuration to use the OpenDNS servers (which are 208.67.222.222 and 208.67.220.220)

Only access "important" (i.e. your online banking, or anything else involving money) sites via SSL, and don't just check that the padlock icon is in the browser status bar, view the certificate and make sure it is valid.

Note to Robert McMillan: in the context used in your article, "owned" is normally spelt "pwn3d".

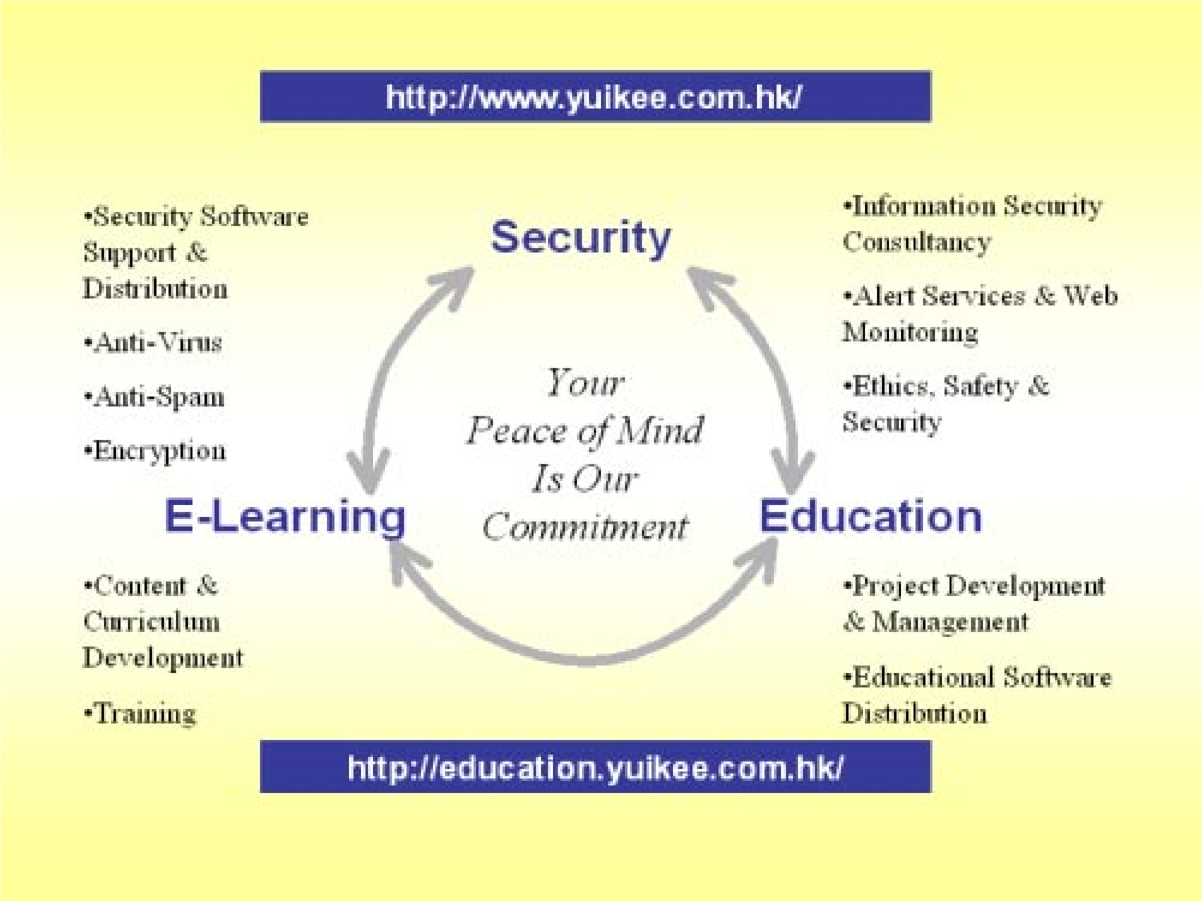
More Information

Hong Kong ISPs: patch your servers against DNS-exploits now!
Exploit code for Kaminsky DNS bug goes wild

DNS attack writer a victim of his own creation
Apple skewered over missing DNS patch
Exploit code targets Mac OS X, iTunes, Java, Winzip...
World's biggest ISPs drag feet on critical DNS patch
Researcher's hypothesis may expose uber-secret DNS flaw
Vendors form alliance to fix DNS poisoning flaw
DoxPara Research
OpenDNS | Providing a Safer and Faster Internet

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/


http://www.yuikee.com.hk/
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
Security
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/