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

Yui Kee Computing Ltd.

Newsletter

July 2005

Contents

Incident Update

- Wed Jun 1 00:32:56 2005 TREND: WORM_MYTOB.BI Medium
- Wed Jun 1 01:47:35 2005 FSC: Bagle downloaders spammed 2
- Wed Jun 1 11:02:27 2005 CA: Mytob.DO Medium
- Wed Jun 1 11:46:56 2005 CA: Glieder.AG Medium
- Thu Jun 2 22:32:38 2005 CA: Mytob.DR Medium
- Thu Jun 2 23:18:42 2005 CA: Mytob.DT Medium
- Fri Jun 3 20:47:08 2005 TREND: TROJ_SMALL.AHE Medium
- Fri Jun 3 20:47:08 2005 TREND: WORM_BOBAX.P Medium
- Fri Jun 3 20:47:08 2005 CA: Win32.Mytob.DU Medium
- Wed Jun 8 00:02:44 2005 CA: Mytob.DS!Worm Medium
- Wed Jun 8 09:17:31 2005 CA: Mytob.EC Medium
- Mon Jun 27 16:02:02 2005 CA: Win32.Mytob.X Medium

Yui Kee On TV – Part 2

Last month we mentioned a n RTHK documentary about spam, which aired on 11th July. The programme can now be viewed online at the RTHK website:
http://www.rthk.org.hk/rthk/tv/hkcc/20050711.html
The programme is mainly in Cantonese (except comments from our Chief Consultant, Allan) with Chinese subtitles.

Eliminate Rodent Nuisance

Mark Burnett encourages us to address basic insecurities on all our systems. He particularly targets our current SMTP email, and advocates replacing insecure protocols like telnet and ftp with ssh and sftp, “Who wants to be backwards compatible with insecurity anyway?”, he says.

Full article:

http://www.theregister.com/2005/07/01/rats_in_the_security_world/

No Avoiding Full Disclosure

Vendors, such as Microsoft, have sometimes released security patches without specifying exactly what is being fixed. The vendor justifies this by saying that it is to prevent the bad guys exploiting the flaw on unpatched systems. Security analysts counter this, saying that, theoretically, comparing the patched and unpatched software, and reverse-engineering the differences will reveal flaw.

It sounds easy, in theory, but all security is a trade-off – how much time does not publishing the full details buy us? Halvar Flake decided to find out for last month’s critical flaw in Internet Explorer, and was able to pinpoint the PNG vulnerability within 20 minutes.

More information:

http://www.theregister.com/2005/07/01/reverse_engineering_patches/

Longest Day

The 31st December will be the longest day of 2005, as it will have 86,401 seconds. The International Earth Rotation And Reference Systems Service (IERS) has announced a positive leap second, so the last second of the year will be 2005 December 31, 23h 59m 60s. The IERS monitors the rotation of the earth, and issues leap seconds to accommodate variations, when measured against the most accurate atomic clocks.

More information:

http://hpiers.obspm.fr/eop-pc/

Patent Absurdity

By Richard Stallman

URL: http://news.zdnet.com/2100-9593_22-5754104.html

Commentary--Next month, the European Parliament will vote on the vital question of whether to allow patents covering software, which would restrict every computer user and tie software developers up in knots.

Many politicians may be voting blindly--not being programmers, they don't understand what software patents do. They often think patents are similar to copyright law (except for some details), which is not the case.

For example, when I publicly asked Patrick Devedjian, then the minister for industry, how France would vote on the issue of software patents, he responded with an impassioned defense of copyright law, praising Victor Hugo for his role in the adoption of copyright.

Those who imagine effects like those of copyright law cannot grasp the real effects of software patents. We can use Hugo as an example to illustrate the difference between the two.

A novel and a modern complex program have certain points in common: each is large and implements many ideas. Suppose patent law had been applied to novels in the 1800s; suppose states such as France had permitted the patenting of literary ideas. How would this have affected Hugo's writing? How would the effects of literary patents compare with the effects of literary copyright?

Consider the novel "Les Misérables," written by Hugo. Because he wrote it, the copyright belonged only to him. He did not have to fear that some stranger could sue him for copyright infringement and win. That was impossible, because copyright covers only the details of a work of authorship, and only restricts copying. Hugo had not copied “Les Misérables,” so he was not in danger.

Patents work differently. They cover ideas--each patent is a monopoly on practicing some idea, which is described in the patent itself.

Here's one example of a hypothetical literary patent: Claim 1: a communication process that represents, in the mind of a reader, the concept of a character who has been in jail for a long time and becomes bitter towards society and humankind.

Claim 2: a communication process according to claim 1, wherein said character subsequently finds moral redemption through the kindness of another.

Claim 3: a communication process according to claims 1 and 2, wherein said character changes his name during the story.

If such a patent had existed in 1862 when “Les Misérables” was published, the novel would have infringed all three claims--all these things happened to Jean Valjean in the novel. Hugo could have been sued, and would have lost. The novel could have been prohibited--in effect, censored--by the patent holder.

Now consider this hypothetical literary patent:

Claim 1: a communication process that represents, in the mind of a reader, the concept of a character who has been in jail for a long time and subsequently changes his name.

“Les Misérables” would have infringed that patent too, because it also fits the life story of Jean Valjean.

These patents would all cover the story of one character in a novel. They overlap, but they do not precisely duplicate each other, so they could all be valid simultaneously--all the patent holders could have sued Victor Hugo. Any one of them could have prohibited publication of “Les Misérables.”

You might think these ideas are so simple that no patent office would have issued them. We programmers are often amazed by the simplicity of the ideas that real software patents cover--for instance, the European Patent Office has issued a patent on the progress bar, and one on accepting payment via credit cards. These would be laughable if they were not so dangerous.

Other aspects of “Les Misérables” could also have fallen foul of patents. For instance, there could have been a patent on a fictionalized portrayal of the Battle of Waterloo, or a patent on using Parisian slang in fiction. Two more lawsuits.

In fact, there is no limit to the number of different patents that might have been applicable for suing the author of a work like “Les Misérables.” All the patent holders would claim they deserved a reward for the literary progress that their patented ideas represented--but these obstacles would not promote progress in literature. They would only obstruct it.

However, a very broad patent could have made all these issues irrelevant. Imagine patents with broad claims, like these:

- Communication process structured with narration that continues through many pages.

- A narration structure sometimes resembling a fugue or improvisation.
- Intrigue articulated around the confrontation of specific characters, each in turn setting traps for the others. Who would the patent holders have been? They could have been other novelists, perhaps Dumas or Balzac, who had written such novels--but not necessarily.

It isn't necessary to write a program to patent a software idea, so if our hypothetical literary patents follow the real patent system, these patent holders would not have had to write novels, or stories, or anything--except patent applications. Patent parasite companies--businesses that produce nothing except threats and lawsuits--are growing larger.

Given these broad patents, Hugo would not have reached the point of asking what patents might get him sued for using the character of Jean Valjean. He could not even have considered writing a novel of this kind.

This analogy can help non-programmers to see what software patents do. Software patents cover features, such as defining abbreviations in a word processor or natural order recalculation in a spreadsheet.

They cover algorithms that programs need to use. They cover aspects of file formats, such as Microsoft's new formats for Word files. The MPEG 2 video format is covered by 39 different US patents.

Just as one novel could infringe many different literary patents at once, one program can infringe many different patents at once. It is so much work to identify all the patents infringed by a large program that only one such study has been done.

A 2004 study of Linux, the kernel of the GNU/Linux operating system, found that it infringed 283 different U.S. software patents. That means each of these 283 different patents covers a computational process found somewhere in the thousands of pages of source code of Linux.

The text of the directive approved by the council of ministers clearly authorizes patents covering software techniques.

Its backers claim the requirement for patents to have a "technical character" will exclude software patents--but it will not. It is easy to describe a computer program in a "technical" way, the boards of appeal of the European Patent Office said.

The board is aware that its comparatively broad interpretation of the term "invention" in Article 52 (1) EPC will include activities so familiar that their technical character tends to be overlooked, such as the act of writing using pen and paper. Any usable software can be "loaded and executed in a computer, programmed computer network or other programmable apparatus" in order to do its job, which is the criterion in article 5 (2) of the directive for patents to prohibit even the publication of program.

The way to prevent software patents from bollixing software development is simple: don't authorize them. In the first reading, in 2003, the European parliament adopted the necessary amendments to exclude software patents, but the council of ministers reversed the decision.

Citizens of the EU should phone their MEPs without delay, urging them to sustain the parliament's previous decision in the second reading of the directive.

biography

Richard Stallman launched the GNU operating system (www.gnu.org) in 1984 and founded the Free Software Foundation (fsf.org) in 1985. Gérald Sédrati-Dinet devised the examples in this article.

http://news.zdnet.com/2102-9593_22-5754104.html?tag=printthis

Sasser Suspect on Trial… Sentenced

Sven Jaschan, the German teenager responsible for the Sasser worm, went on trial behind closed doors near the beginning of July. Three days later, he had been sentenced to 30 hours community service, and less than two years probation. His confession and the fact that he was legally a juvenile at the time the worm was released contributed to the light sentence.

The Sasser worm infected thousands of computers in May 2004. Jaschan also authored the Netsky worm. One of Jaschan's viruses, Netsky.P, is still number 4 in F-Secure’s virus statistics, almost 16 months after it was released.

Two people who contacted Microsoft’s Anti-Virus Reward Program to identify Jaschan as Sasser’s creator have received a substantial reward.

●	$250,000	Microsoft’s reward to Sasser informants.
●	$157,000	Estimated damage caused by Sasser at 143 plaintiffs who contacted authorities.
●	$0	Fine and Damages paid by Jaschan.

Sophos conducted a web poll of more than 550 business PC users and found 78% believed the sentence was too lenient. "With almost 80% of those surveyed saying Jaschan's sentence was too lenient, it seems that many computer users aren't convinced justice has been served," said Carole Theriault, security consultant at Sophos. "Perhaps even more interesting about the Jaschan sentencing is Microsoft splashing out US $250,000 to the two unidentified people who helped track Jaschan down - especially when speculation hints that these people are teenagers who may have had some involvement with Jaschan. It's good to see Microsoft taking strong action against such crimes, but it might struggle if it has to shell out big bucks for every virus writer who gets arrested."

A virus Jaschan wrote, W32/Netsky-P, is still one of the commonest viruses today, 16 months after it was released.

Jaschan now works at a German information security company, which, apparently valuing publicity over reputation, offered him a job after his arrest.

More information:

http://www.theregister.com/2005/07/05/sasser_trial_begins/

http://www.spiegel.de/netzwelt/politik/0,1518,364256,00.html

http://www.theregister.com/2005/07/08/sasser_sentencing/

http://www.f-secure.com/weblog/archives/archive-072005.html - 00000594

http://www.theregister.com/2005/07/08/sasser_snitch_reward/

http://www.sophos.com/virusinfo/articles/sasserpoll.html

http://www.sophos.com/virusinfo/articles/sasserfree.html

Pakistan Returns to the Internet

The Southeast Asia-Middle East-Western Europe-3 (SEA-ME-WE3) cable, which carriers most of Pakistan’s Internet traffic, has been repaired ten days after it was damaged.

http://www.theregister.com/2005/07/08/pakistan_cable/

Commwarrior Continues Spread

Possibly the most boring virus outbreak in recent years, Commwarrior, which infects Symbian Series 60 mobile devices and can spread by Bluetooth and MMS has now been reported from the UK.

The situation is reminiscent of the early days of PC viruses – there are a handful of viruses that are spreading slowly and causing almost no damage. Commentators are saying there is no threat from mobile viruses, or the threat has been over-hyped by vendors. If the same pattern is followed, we will see increasing market penetration of highly-capable mobile devices, and a sudden, massive outbreak that causes massive disruption. Or perhaps we should learn from past experience?

http://www.f-secure.com/weblog/archives/archive-062005.html - 00000583

In Case of Emergency

The U.K. East Anglian Ambulance Service are promoting the idea of storing the word "ICE" in your mobile phone address book, and against it enter the number of the person you would want to be contacted "In Case of Emergency".

In an emergency, ambulance or hospital staff can contact your next of kin quickly simply by looking for the ICE entry.

F-Secure reports that a hoax advising against this idea has already emerged. The hoax wrongly suggests that a virus could misuse the ICE entry. Viruses that misuse every entry in the phone book already exist, an ICE entry does not make this any worse.

More information:

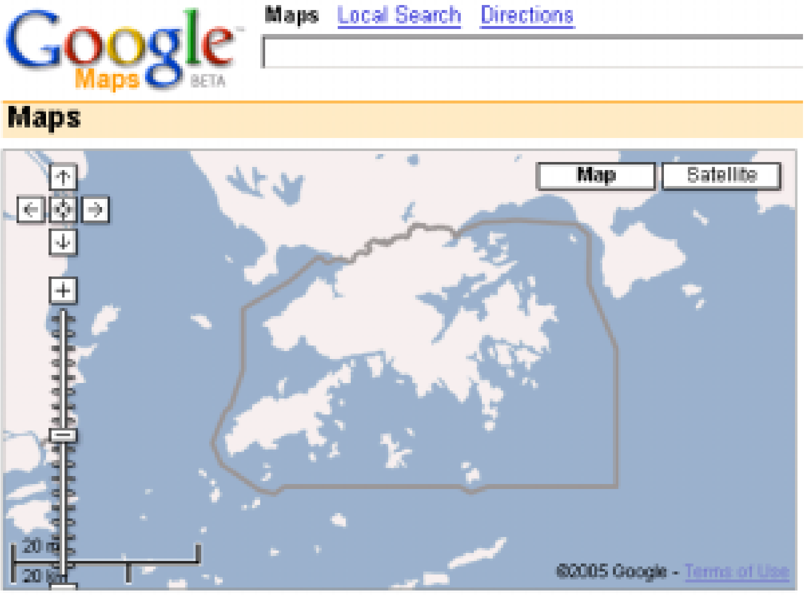
http://www.theregister.com/2005/07/14/ice_mobile/

http://www.eastanglianambulance.com/content/news/newsdetail.asp?newsID=646104183

http://www.f-secure.com/weblog/archives/archive-072005.html#00000602

http://s408.link.sophos.com/icehoax?pl_id=9

Where's HK Island, Google?



Google UK has previously been criticized for not showing parts of the world outside the British Isles and North America on its map site http://maps.google.co.uk/. Although that has mostly been corrected, and the boundary of the SAR is shown, Hong Kong Island itself is missing. Residents will be pleased to know that the island does exist on the satellite photos.

More on Google's Mapping Abilities:

http://www.theregister.com/2005/07/15/google_spots_jesus/

Sophos Anti-Virus certified to detect 100% of spyware in Checkmark tests

Independent research and test center West Coast Labs has announced that Sophos Anti-Virus for Windows XP has been awarded the certification Checkmark for detecting 100% of the spyware in their rigorous tests.

The certification confirms Sophos's expertise in protecting businesses against the spyware threats and joins existing awards that have demonstrated the Sophos product suite's expertise in detecting and disinfecting all known in-the-wild viruses and Trojan horses.

By passing West Coast Labs' stringent Checkmark spyware certification test, Sophos has again demonstrated its effectiveness in protecting business against all kinds of malicious content.

"Organizations are demanding anti-spyware protection that is purpose-built for business and Sophos's award of the Checkmark Spyware Certification confirms the excellence of their solution," said Chris Thomas, Operations Director at West Coast Labs. "We're delighted to report that Sophos's anti-virus product detected 100% of the spyware including password stealers, crackers, financials, keyloggers, backdoors, downloaders and proxys in West Coast Labs' test suite, without causing a single false alarm."

West Coast Labs, an independent research and test center, developed the Checkmark system. It provides a reliable means of authenticating products and certifying those of the highest quality.

More information:

http://www.sophos.com/virusinfo/spyware/

http://www.sophos.com/companyinfo/news/spywarechckmrk.html

UK Regulator Asks for Power to Stop Spam

The enforcer of the UK's anti-spam laws, the Office of the Information Commissioner (ICO), has received about 600 spam complaints during the last year, but it has taken no legal action.

However, the ICO has not been idle, it also oversees Personal Data Protection issues, and it has prosecuted 12 cases under that law.

About half of the spam complaints received were outside of the scope of the regulations, and the ICO also did not follow-up cases involving overseas spammers, or spammers who could not be identified. The ICO had the most success in encouraging reputable companies to improve their practices.

However, the ICO was ineffective against less scrupulous companies who routinely ignored the warning letters. They could also delay action against them for up to a year by simply appealing against the Enforcement Notice. The ICO is lobbying the Department of Trade and Industry for powers to stop spammers immediately, and for better information-gathering powers.

Comment by Allan Dyer:

Hong Kong's Legislators should look carefully at the UK's experience when developing our legislation. Key areas are:

1. Why are so many of the complaints outside the scope of the regulations? There is some kind of mismatch between what people need or expect, and what the regulations can do.
2. The law is successful in encouraging reputable companies to behave responsibly.
3. There needs to be sufficient investigation and enforcement power to pursue those who flout the regulations in a timely manner.

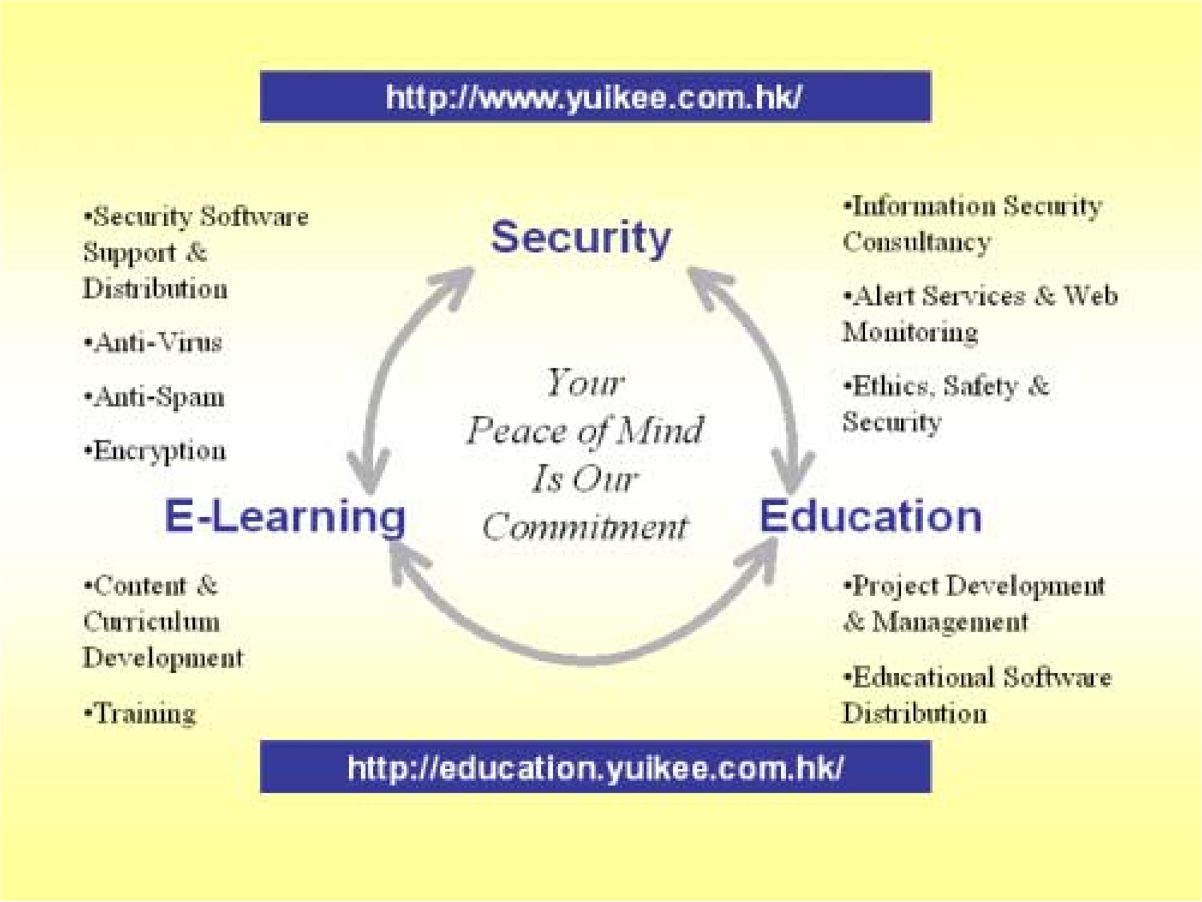
More information:

http://www.out-law.com/page-4714

http://www.informationcommissioner.gov.uk/cms/DocumentUploads/very%20final%20ICO%20Annual%20Report%202005%20HC%20110.pdf

http://www.theregister.com/2005/07/20/uk_regulator_seeks_power_to_stop_spammers/

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/



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

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/