Yui Kee Computing Ltd.

Newsletter

January 2008

Contents

UK Government Issues Guidelines on Hacking Tools

<web-link for this article>

The Crown Prosecution Service in the UK has published guidelines about how courts should interpret the updated Computer Misuse Act, which includes the controversial offence of "making, supplying or obtaining articles" for use in other offences, in other words, controlling "hacking" tools. Security professionals pointed out the difficulty of categorising tools as good or bad, and the implications this would have for the "good guys" when the law was proposed. The guidelines will greatly influence how the courts apply the law once it comes into effect.

The guidelines do specifically mention that there is a legitimate industry concerned with computer security that "generates 'articles'" for testing and audit purposes, and that prosecutors should ascertain whether there was criminal intent. Under supplying, or offering to supply, the guidelines advise considering the following factors to determine the likelihood that the article would be used for illegal purposes:

- Was it developed primarily, deliberately and for the sole purpose of committing an offence?
- Is it available on a wide-scale commercial basis and sold through legitimate channels?
- Is it widely used for legitimate purposes?
- Does it have a substantial installation base?
- What was the context of its use compared to its intended purpose?

These factors rule out the most ridiculous potential mis-applications of the law. For example, Perl, or the text-editor used to create a malicious Perl script, would not be considered 'articles' because they were not built for that sole purpose, they are widely used for legitimate purposes, and may have a substantial installation base. Makers of general-purpose programming languages and editors can probably rest easy in the knowledge they will not be prosecuted if their tools are used for illegal purposes.

However, creators of more specialised tools should be more worried, particularly if they release the tool as open source. Why does commercial sale affect the likelihood of a tool being used for crime? What is a legitimate channel? Is a web-sale more or less "legitimate" than a shop sale? When the installation base is calculated, is it determined for the particular version in question, or all versions of the tool? For example, the popular Nessus tool releases new plugins to paying users seven days before they are released for free. The paying users are, undoubtedly, a much smaller installation base than the free users, does this affect the likelihood of Nessus being used for illegal purposes, and therefore open the developers to prosecution in the UK?

The guidelines strongly discourage Full Disclosure - publishing a description of a security vulnerability with a code example of how to exploit it would open the author to prosecution - the code example would clearly have the intention to subvert the security of the vulnerable system. In the past, some developers have refused to acknowledge or fix vulnerabilities, saying that they are "only theoretical" and "not practical" until a researcher has provided a working code example. It seems to be very unwise to do this in the UK now, so we can expect a negative effect on the security of common products.

More Information

Hacking tool guidance finally appears
UK gov sets rules for hacker tool ban
Computer Misuse Act 1990
German Government Shoots Self in Anti-Hacking Foot
Home Office pushes tough anti-hacker law
Police and Justice Bill - dual use "hacker tools" - has the Government finally seen sense ?
Nmap - Free Security Scanner For Network Exploration & Security Audits
Tenable Network Security: Nessus Plugings

Jeremy Clarkson Demonstrates Personal Data Leak Threat

But he was trying to prove the opposite.

<web-link for this article>

Outspoken BBC TV presenter Jeremy Clarkson wrote a column in the UK Sun newspaper saying that the public outcry about the loss of unencrypted CDs containing child benefit details, including bank details of 25m people, was a lot of fuss about nothing. To back up his claim, he included his own bank account number, sort code, and clues to his address, saying that the worst that could happen was that someone could pay money into his account.

He was dramatically proved wrong when an unknown person set up a Direct Debit from his account to the charity Diabetes UK, resulting in the transfer of £500. In another column, he has retracted his claim, saying, "I was wrong and I have been punished for my mistake." He has also advocated tough new measures to prevent Personal Data disclosure, saying, "Contrary to what I said at the time, we must go after the idiots who lost the discs and stick cocktail sticks in their eyes until they beg for mercy." Clarkson should be applauded for his willingness to admit when he is wrong.

However, Clarkson is best-known for his knowledge, and love of, cars, not for his expertise in Information Security, and he is still missing a important point: the financial loss was only possible because there was also negligence at his bank. Disclosure of personal data is not just about financial loss, there are many situations where it can cause even more serious harm to the victim(s), but this is primarily a financial example. The bank failed to verify that the direct debit instruction was issued by Clarkson, so the bank is responsible.

This is a reflection of how the information revolution is changing our society, and institutions, like banks, are failing to adapt. We have long been used to using our written signature on important transactions, even though signatures can be forged and challenged. Additional procedures increased the difficulty of crime: banks expect you to know the account name and number, and provide pre-printed cheques for your convenience - making a non-preprinted cheque immediately suspicious. There is an obvious cost pressure towards skipping signature checks - after all, the name and number can be checked automatically, but a signature must be manually verified, and who else would know the matching account name and number? Unfortunately, nowadays, everyone; because of the potential for massive personal data disclosures.

Fortunately, there is an easy solution; the banks and financial institutions have been quietly ignoring the problem, or trying to transfer the blame and cost to the customer. Therefore, the Regulators should put the responsibility firmly back with the bank, assuming that the blame lies there until proven otherwise, and imposing punitive penalties for lapses. This will give banks the right incentive to develop and promote user-friendly secure authentication mechanisms.

More Information

Clarkson's 'steal my ID' stunt backfires
Clarkson stung after bank prank
"I was wrong and I have been punished for my mistake"

Fort Datacentre?

<web-link for this article>

A recently revealed incident that occurred last October has raised the question of whether most datacentres are adequately protected against armed robbery. In the incident, armed thieves entered a datacentre in Chicago, and coerced the lone IT working into scanning his fingerprint and revealing his PIN to allow them full access to the facility.

Security blogger Christopher Faulkner, said that the incident shows how the majority of IT managers have inadequate measures in place to counter the threat posed by violent burglars. An alternative view would question whether the majority of datacentres have assets that are attractive to armed robbers. Armed robbery is a high-risk crime, so it should offer high rewards. Datacentres have hardware and data assets. In most cases, the hardware is generic equipment that is falling in price, and the specialised hardware might be valuable, but it will be traceable and hard to sell. The data may be valuable, but the value might be dependent on the theft being concealed - for example, credit card numbers that could be misused until the bank cancels them. There would probably be denial of service aspects, but those should be addressed by disaster recovery plans. It might be appropriate to implement full-disc encryption, so that, even if the servers are stolen, the data is inaccessible. This also protects the data from copying by unauthorised staff with access to the datacentre.

So, for most organisations, "adequate measures" are a policy that armed robbers should be given what they want, and the Police called afterwards. Introducing armed guards into the datacentre of an otherwise unarmed organisation is greatly increasing the risk of death or injury, and increasing the costs of security unnecessarily. As always, security is about balancing costs against protection.

More Information

Datacenter security worries raised
Are You Wasting Money on Security?

Pole Kid in Point Hack

<web-link for this article>

A Polish teenager has been arrested for using a home-made device to change the points on the Lodz tram network, derailing four trams and injuring twelve people. Police say that the fourteen-year-old trespassed in tram depots to gather information he used to build or modify a device like a TV remote control that could control all the junctions on the system.

Transport staff immediately suspected outside interference on 8th January when a driver attempting to steer his vehicle to the right was involuntarily taken to the left, resulting in the rear car jumping the rails and colliding with another passing tram. A Police search found the device, a school exercise book recording his research on the trams network and good junctions to control, and square-ended keys of the type often used in transport networks for opening "staff only" doors. The boy will face charges of endangering public safety in a juvenile court.

The junctions on tram networks are often controlled by the drivers, and not by a centralised system. An article in Gazeta Wyborcza confirms that Lodz tram junctions are, indeed, infra-red controlled, and might even be affected by an unmodified remote control in the hands of a passenger.

People in Hong Kong may wonder whether the city's tram network is similarly vulnerable.

More Information

Schoolboy hacks into city's tram system
Polish teen derails tram after hacking train network
14-latek wykolejał tramwaje (photo)
14-latek wykolejał tramwaje (arrest photo)
Pilot od telewizora w Łodzi może wszystko

Fine for DNS Zone Transfer $53,000 in North Dakota

<web-link for this article>

Anti-spam activist David Ritz used the host -l command to effect a zone transfer from the servers of Sierra Corporate Design, a North Dakota business run by Jerry Reynolds, and subsequently published the information, along with whois data. Sierra sued Ritz for unauthorized access, trespass to chattels and publication of the information obtained.

In a civil case, Judge Cynthia Rothe-Seeger found that the use of the "unauthorized" because it was not performed by a secondary authoritative domain name server or a network administrator for the system, and was therefore outside the *intended* use of the command. The zone data included the internal zone structure of Sierra, with private host names, that could not be obtained from any (other) public source. Judge Rothe-Seeger found that Ritz publishing the information "created a grave security risk for Sierra". The Judge noted that Ritz had ill-will and malice against Sierra, as a suspected spammer, but found, "those suspicions do not justify violations of the law nor trespass". She awarded Sierra $2930 in actual damages, $50000 in exemplary damages, allowed Sierra to recover lawyers fees and fined Ritz $10000 for an associated contempt charge. Ritz may also face criminal charges over the alleged offences.

The focus of attention for system administrators will be that Judge Rothe-Seeger has found that using an ordinary Unix tool, host, with an ordinary switch, -l, to access unprotected information on a publicly-accessible server without specific authorisation is illegal. The Judge found that the information was not "publicly accessible" because it was not the intended use of a zone transfer. Think carefully before you touch a command-line!

More Information

Anti-spammer fined $60K for DNS lookup 'hack'
Findings of Fact, Conclusions of Law, and Order for Judgment
Sierra Corporate Design Inc. v. David Ritz
North Dakota Judge Gets it Wrong

Clearswift Blocks 100% of Spam... and 100% of Other Email Too

<web-link for this article>

A domain name problem at email and web-filtering company Clearswift resulted in about 5% of their customers having all email blocked, starting early 23rd January. This coincides with the last update time of 03:12:53 that day for the mimesweeper.biz domain, used for routing the email to be filtered. The whois record for the domain shows that it expired on 12th December 2007, leading to speculation that a failure to renew the domain led to the problem when the grace period expired. Some customers have worked around the problem by adding addresses to their mail configuration files, allowing messages to take alternate routes. Alyn Hockey, Clearswift's director of product management, was unsure what caused the domain name failure.

More Information

Domain name gaffe launches Clearswift clients into e-mail panic
Whois at Sam Spade.org

Dawn Raid on Aberdeen Teen Hacker

<web-link for this article>

A 14-year old boy was arrested at his home in Old Main Street, Aberdeen, Hong Kong, for illegal access to school computers at 7am on 23rd January. He accessed a password-protected teacher-student exchange forum, but the investigation showed no sensitive or secret information had been stolen and he claimed to have done it for "fun", according to Chief Inspector Kenny Wong Tak-cheung. He also claimed that a classmate taught him the procedure. Police are expected to arrest the classmate. The maximum penalty for this crime in Hong Kong is five years jail.

More Information

Boy, 14, held for computer hacking

First Virus Writer Arrest in Japan

<web-link for this article>

Japanese Police have arrested three men in a case involving the creation and distribution of malware called Harada in the Japanese media. Harada is thought to be related to the Pirlames Trojan horse. The malware displays images of popular anime characters while deleting MP3 and movie files. However, reports indicate that the three are being charged, not with the destruction of data, but with copyright violation for using the anime images, due to a lack of "applicable cybercrime laws"!

However, this does not match with other information about cybercrime law in Japan. In most jurisdictions, including Hong Kong, specifically writing a virus is not illegal. It would be crazy to make such a law: the formal definition of a computer virus covers far too much, to take an ancient example, a bootable DOS disc with the diskcopy.exe program is a functional computer virus - should we arrest Bill Gates for writing DOS? This makes Graham Cluley's remark about

this case, "It isn't illegal to write viruses in Japan," odd, does Mr Cluley think a law that would make many ordinary programmers into criminals is advisable? Instead, good laws usually refer to intent and damage. In Hong Kong, intentionally making unauthorised changes to programs or data is categorised as criminal damage. This makes spreading a computer virus illegal (it modifies other programs), and also covers the intentional damage to data caused by Harada.

Does Japan have a law that could be applied? Speaking at the 2004 AVAR Conference in Tokyo, Takashi Garcia SATO, Assistant Director, Superintendent, Cybercrime Division of the National Police Agency, Japan, gave statistics for three types of cybercrime in Japan: unauthorised computer access, crime against computer / data and internet crime. As a specific example of a crime against computer / data, he reported the 2004 March, Hyogo case where a criminal deleted hospital's data including 500 patients' name, address and disease name and obstructed business of the hospital because he received a caution in the hospital and got angry.

Both the Hyogo case and the current Harada case feature the intentional destruction of data without a clear profit motive, so it would appear that Japan *does* have an applicable law. However, it may be that the specific wording of the law makes it difficult to be applied where the damage is intermediated by malware. It would be interesting to hear more.

25th January 2008

Graham Cluley has clarified that his quote was poorly crafted if it's suggestion that he thinks making virus-writing illegal is a good idea, and it's better to get the bad guys with the usual data destruction / unauthorised access laws. The Sophos website has been updated.

More Information

Virus writers charged with copyright violation
First virus writer arrested in Japan.. for breaching copyright
Computer Secutiry Situation in Japan (Report from National Police Agency Japan)
コンピューターウイルス：作成者、国内で初逮捕　京都府警
Crimes in Japan in 2006
The Legal Framework - Unauthorized Access To Computer Systems Penal Legislation In 44 Countries
Arrests and Consultations of Cybercrime in 2003
Graphic Japanese Trojan attacks P2P file-sharing pirates

Unsubscription Information

To subscribe, send an email to Maiser@yuikee.com.hk with subscribe newsletter in the message body. The Subject can be anything. Send the subscription email now. If successful, you will receive a welcome message.

To unsubscribe, send an email to Maiser@yuikee.com.hk with unsubscribe newsletter in the message body. The Subject can be anything. Send the unsubscription email now. If successful, you will receive a farewell message.

You can only subscribe or unsubscribe the address you are emailing from. If you need to add or remove another address from the list (eg. you have changed email addresses and want to unsubscribe the old address), or you have any other problems concerning the operation of the list, please contact the Postmaster.

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/