Yui Kee Computing Ltd.

Newsletter

September 2007

Contents

Hong Kong Liberal Party Can Count but Sin Chung Kai uses Wife's Name in Password

<web-link for this article>

Swedish security researcher Dan Egerstad has published a list of one hundred passwords of Government-related email accounts, including Legislative Council members. Egerstad claimed he was able to get the passwords because users of the accounts were misusing a common security application in a way that allowed him to perform a man-in-the-middle attack. He said that the vendor of the software provided ample warnings against using it in that manner.

Apart from inadvertently mis-using a security application, the passwords reveal a range of knowledge or attitudes to password choice. For example, tinyan at the Hong Kong Liberal party uses '12345678', which is possibly better than miriamlau's '123456'.

But at least we can expect the Democratic Party to benefit from the advice of their LegCo member for the IT Functional Constituency, and therefore choose more secure passwords? Apparently not, as twk has chosen 'password'. Perhaps this is not too surprising, as Sin Chung Kai, the LegCo member in question, has a password consisting of his wife's name and what might be a date. At least we known when to send his wife birthday cards.

The list contains nineteen Hong Kong-related addresses and passwords, mostly for political parties and LegCo members, though there is one for the Hong Kong Government Information Service Department.

Owners of these accounts should check that their procedures for accessing them are in accordance with the application vendor's security advice, and then change their passwords immediately. The organisations concerned should review their policies and how they are being enforced.

Please remember that accessing the accounts without authorisation is a criminal offence.

04th September 2007

We have been informed that the affected organisations in Hong Kong have been contacted, and a report has been made to the Hong Kong Police.

The incident must be especially embarrassing for Hon. Sin Chung Kai because his newsletter to IT Functional Constituency voters on 31st August went out under the headline, "More education on information security is needed". We hope he signs up for a course very soon.

30th September 2007

On the 5th September 2007, Hon. Sin Chung Kai issued a statement strongly condemning the actions of the Swedish researcher in a special issue of his newsletter. Sin noted that the actions were likely in breach of Hong Kong law, such as the Telecommunication Ordinance (Chapter 106) Section 27A Unauthorized access to computer by telecommunications; and the Crimes Ordinance (Chapter 200) Section 161 Access to computer with criminal or dishonest intent, and stated that the Hong Kong Police had his full cooperation on the matter. In fact, the stated intent of the researcher was not criminal or dishonest, but it remains to be seen whether there is evidence otherwise.

Our Chief Consultant, Allan Dyer, felt there were wider issues to be addressed and sent Hon. Sin the following email:

"*I think your statement leaves out some very important issues, and I think a fictional scenario might help to illustrate this. Suppose a person walked into an unlocked bank-vault, picked up the largest gold bar they could find and then dropped it in the middle of the bank, in front of all the customers, shouting "look what I've done". The person has done something wrong by entering the vault and moving the gold without permission, but they have highlighted a security problem and haven't actually stolen anything. It would certainly be appropriate for the police to investigate, and search them, to see if they had other valuables from the vault in their pockets, but customers would want to know why the vault was unguarded, what valuables were at risk and what the bank was doing to improve its security. The bank should be accountable for the poor security.*

Your statement does not address the accountability issue. You have made clear the illegality of the security researcher's actions, now let us hear about the Information Security Management of you and your office, specifically:

1. *Why were you and your staff using an insecure method to access your mail? POP3 with simple authentication sends passwords in the clear, the APOP extension is better because it sends the MD5 hash of the password and a timestamp code, although recent research suggests attacks are still possible (see references below). The best solution is probably to tunnel the POP connection over an encrypted session, SSH or SSL (personally, I was tunnelling POP3 over SSH on Windows 3.1, that was a long time ago).*
2. *Although the attack did not involve password guessing, it did reveal how weak some of the passwords are, for example, your staff using 'password', and you using your wife's name. What password policy did you have in place?*
3. *What types of information were at risk? Were these email accounts used for personal correspondence, party business, or Government business? Were any sensitive messages ever stored in these accounts?*
4. *What are you doing to improve the security? Apart from improving your policies and procedures, you should consider regular testing: security audits and penetration tests, give someone the job of looking for these problems before a bad guy does it for free... without telling you!*"

As of the date of publication, a response has not been received from Hon. Sin. Perhaps voters in Hong Kong's IT Functional Constituency can learn about their representative's commitment to practicing what he preaches from this incident.

More information:

DEranged gives you 100 passwords to Governments & Embassies
Hacked: Email inboxes of Indian missions in US and China; NDA, DRDO officials too
Security SNAFU exposes email logins for 100 foreign embassies (and counting)
Vulnerability Summary CVE-2007-1558
APOP vulnerability Apr 02 2007 03:13PM
Mozilla Foundation Security Advisory 2007-15
Sylpheed Security Update Fixes APOP Protocol Information Disclosure Security Weakness
Where NT Stores Passwords
OLEXP: Error Message: A Connection Failure Has Occurred (Error -23012)
POP3 Delivers

Sony will remove rootkit from MicroVault

<web-link for this article>

Following the revalation last month that software supplied with the Sony MicroVault USM-F uses rootkit techniques to hide a directory from the operating system, Sony has announced that it will provide an update without the dangerous technology. Sony claims the problem was in code supplied by a third-party developer from China.

F-Secure, the company that first found the problem, reports that they are helping Sony with the investigation

More Information

Sony to exorcise 'rootkit' from USB drives
Sony is Awake

Appeals Court rejects remedies against Spamhaus

<web-link for this article>

The US Court of Appeals for the Seventh Circuit has set aside an $11M judgement with an injunction that barred the anti-spam organisation Spamhaus from listing either e360 Insight or its principal David Linhardt as a source of spam. However, the original ruling still stands.

In the ruling made by an Illinois court in September 2006, Spamhaus was ordered to pay compensation to e360 Insight, remove the organisation's listing, and post a notice stating that it was wrong to say e360 Insight was involved in sending junk mail. UK-based Spamhaus did not defend the case and the ruling was made in its absence.

Spamhaus, considering itself outside of the American court's jurisdiction, initially ignored the ruling, prompting e360 to ask the court to get Spamhaus's domain suspended. The court denied the request.

The case has prompted some debate about blacklisting, spammers and spam prevention, with Morely Dotes reporting on his policy of blocking, "email from China, Japan, Thailand, Korea, UAE, Turkey, Israel, or numerous other nations which are hotbeds of malicious software, and the proximate sources of most of the spam aimed at us". Such indiscriminate blocking is undoubtedly causing problems, and possibly lost business, for legitimate users around the world. Spamhaus has long offered a much more refined and accountable blacklisting resource.

More Information

Court junks $11m judgment against Spamhaus

Comments on ‘Court junks $11m judgment against Spamhaus’
ICANN claims No Authority to Suspend Spamhaus Domain

F-Secure Internet Security 2008 Introduces Improved Well-Being for PC's

<web-link for this article>

F-Secure Corporation has announced a new milestone in its continued efforts to enable Internet users to take full advantage of the opportunities of their networked lives as easily and safely as possible. With the new F-Secure Internet Security 2008 solution, the company is introducing Online Well-Being as the primary way for PC users to experience data security, as opposed to the traditional threat and fear-oriented approaches the industry has used.

Today, networked living presents PC and smartphone users with incredible opportunities for creativity, social interaction, entertainment, information access, management of personal memories and conducting business. Users increasingly wish to take full advantage of these opportunities, without needing to worry about viruses, network attacks or other malicious phenomena lurking around the Internet.

The simple precaution of using the new F-Secure Internet Security 2008 solution with its improved level of security will enable consumers and small businesses to enjoy the benefits of global networks without fear and nagging worries. The new solution keeps the PC healthy and free from malicious applications with the help of a number of well-integrated and intelligent security features. The solution is specifically designed to require minimal user interaction, and removes the need to separately maintain and update several separate security programs.

The solution includes a 12-month subscription to a fully automated and continuous update service from the F-Secure Security Labs. The proven speed and reliability of this update service ensures a user's PC stays immune to new and evolving threats that continuously target computers that do not have the latest security updates. Moreover, the product includes a unique proactive protection technology, F-Secure DeepGuard™, which provides a very effective additional line of defense during those crucial first hours when no definition-based identification is yet available to protect against new unknown threats. DeepGuard in effect reduces the response time to zero.

The new solution also uses less computer resources than before, thus improving the overall performance of the system. This translates into improved user experience, enabling users to focus more intensively on the important activities in their networked lives. It also features improved parental controls with new categories of controlled Web content and a safe Internet list (so-called whitelist of Web sites). To better protect against fake Web sites designed to fool Web users to disclose their private information, such as fake bank sites, the anti-phishing feature has been improved, including better detection of emails that pretend to be from financial or other trustworthy institutions.

"Security is no longer defined in terms of fear, but the new measure is enablement and opportunity. Our task is to enable our customers to soar with the possibilities of the Net, leaving their security worries to be handled by our professional service" says Ari Alakiuttu, Vice President of Products and Services at F-Secure Corporation.

F-Secure Internet Security 2008 is available from Yui Kee and other F-Secure channels. The solution provides protection for up to three PC's in the same household, supports Windows Vista, and has a localised user interface and electronic user manual in 25 different languages. The solution also helps users take care of the well-being of their most personal computer - the smartphone - by including a free trial version of the F-Secure Mobile Anti-Virus solution for Symbian and Windows Mobile smartphones.

SSH Tips and Tricks: Denying shell access for SFTP Accounts

<web-link for this article>

If you have accounts that are used only for file transfer, it is good practice to limit their access to services, following the principle of least privileges. In the SSH Server configuration, this can be done by denying remote command, terminal and tunneling access for listed users or groups of users (for details, see SSH Tectia Server Administrator Manual, section 7.1.2).

However, sometimes there are many ways to access a system in addition to ssh, and it can be desirable to deny shell access on system level, e.g. by setting the login shell to /bin/false or /sbin/nologin or some other program that is listed in the system list of shells but does not start a shell. Remember that the tunnelling restrictions still need to be done in the ssh-server-config.xml. But can the user transfer files, if the shell is set to /bin/false or similar?

The default behavior in the SSH Tectia Server is to run the file transfer server for an SFTP session through the user's shell. Thus, in the above scenario, the file transfer with SFTP will not work. But starting from SSH Tectia Server version 5.3.2, it is possible to configure the SFTP subsystem to be executed directly and not through the user's shell. This can be done using the new exec-directly="yes" argument for the SFTP subsystem:

```
<subsystem type="sftp"
        application="sft-server-g3"
        action="allow"
        exec-directly="yes">
</subsystem>
```

This option is available on the Unix and Linux platforms. The downside of executing the SFTP server directly, and not through the shell, is that possible shell initialization files (for non-interactive shells) will not be read. Also, user will not be able to connect to SSH Tectia Server using OpenSSH scp.

More Information

SSH Tectia Server 5.3 User Documentation

Fujacks Worm Author Jailed and Rewarded

<web-link for this article>

Li Jun, the author of the Fujacks worm, and his co-defendants Wang Lei, Zhang Shun and Lei Lei were sentenced by a court in Xiantao, Hubei province in September 2007 to between one and four years in jail with Li receiving the stiffest sentence.

However, just days after the sentences were passed, Li Jun, who had confessed to writing the worm and selling it for over 100,000 yuan, was offered a million-yuan salary job as technology director of Jushu Technology, a firm based in Hangzhou City and one of the victims of the worm. Wang Wanxiong, Li's lawyer, has said that ten companies have offered jobs to Li, whom they regard as a "precious genius."

Graham Cluley, senior technology consultant for Sophos commented, "It's important that the IT community does not send out a message that writing viruses or worms is cool, or a fast track into employment. Li Jun broke the law and infected innocent people's computers and websites, causing financial damage. To reward his criminal act, infamy and bad behaviour with a job offer in the IT industry seems frankly perverse."

More Information

Jailed worm author offered job by victim
Jailed Panda worm author offered job by one of his victims
Four years in a Chinese jail for virus writer who created joss-stick worm
Four charged in Hubei Province over Fujacks Worm
Chinese Police Release Fix by Fujacks Suspect
China jails Panda worm writer for four years

Abuse of .hk Domain Names Falls

<web-link for this article>

The Hong Kong Domain Name Registry (HKDNR) has cited statistics from AbuseButler that show a 85% reduction in the number of reports on .hk spamvertised domains between June and August to show the success of joint efforts of Hong Kong agencies to stamp out abusive domains.

HKDNR has been cooperating with the Office of Telecommunications Authority (OFTA), HK Police Force, Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and other agencies to combat phishing and spamming using .hk domains. Once a .hk domain is verified as being involved with phishing or spamming, HKDNR will suspend it immediately.

HKDNR also claim that implementing the Verified by Visa' and 'Secure Code Verification for Online Payment' methods on their payment gateway for domains has resulted in a 95% drop in registration of spamvertised domain in July 2007.

We can expect criminals to target the least well-managed registries around the world when registering their domains, and they will continue working to exploit the system so the cooperation and effort against this abuse must continue and improve, or these recent improvements will evaporate.

More Information

Combating Phishing and Spamming Sites by HKDNR - Towards a More Secured Local Internet Community!
AbuseButler - Spamvertised Domains

Announcing SSH Tectia Server 5.5 for IBM z/OS

<web-link for this article>

SSH Communications will release a new version of SSH Tectia Server for IBM z/OS early in October. This new version introduces advanced transparent tunnelling features that drastically reduce the cost and time needed to secure FTP file transfers and other data in transit within and between Windows, Unix, Linux, and IBM mainframe environments.

One of the key design goals for the new version was to lower the overall cost of the FTP replacement project. With SSH Tectia, the reduced re-mediation efforts yield significant cost advantages, as the set-up and configuration time is typically measured in hours rather than days or weeks required by other solutions. The new features can be activated system-wide or restricted to specific FTP jobs or user ID's. This makes the product the ideal solution for secure file transfers in complex, heterogeneous environments with Windows, Unix, and Linux platforms, as well as IBM mainframes.

Customers with a current maintenance and support agreement will be able to download this new version from the SSH Customer Download Center.

SSH Tips & Tricks: How Does Checkpoint/Restart Feature Work?

<web-link for this article>

Do you need to transfer large files over an unreliable network link? Then here is a feature for you: Checkpoint/restart is a client-side feature that enables restarting a file transfer from the latest checkpoint instead of starting from the beginning. The feature is included in the SSH Tectia Client with EFT Expansion pack, and it works against servers that have the EFT or Tunneling Expansion Pack, as well as against SSH Tectia Server for IBM z/OS.

The feature works so that the client writes checkpoints to a local file.

The interval of the checkpoints can be configured both in seconds and in bytes. Default is 10 seconds and 10 MB. The checkpoints are enabled by setting the checksum option to 'checkpoint'. For example, the following would write checkpoints every 30 seconds and every 10 MB (default value):

```
$ scpg3 --checksum=checkpoint --checkpoint=s30 largefile user@server:/dest/directory/
```

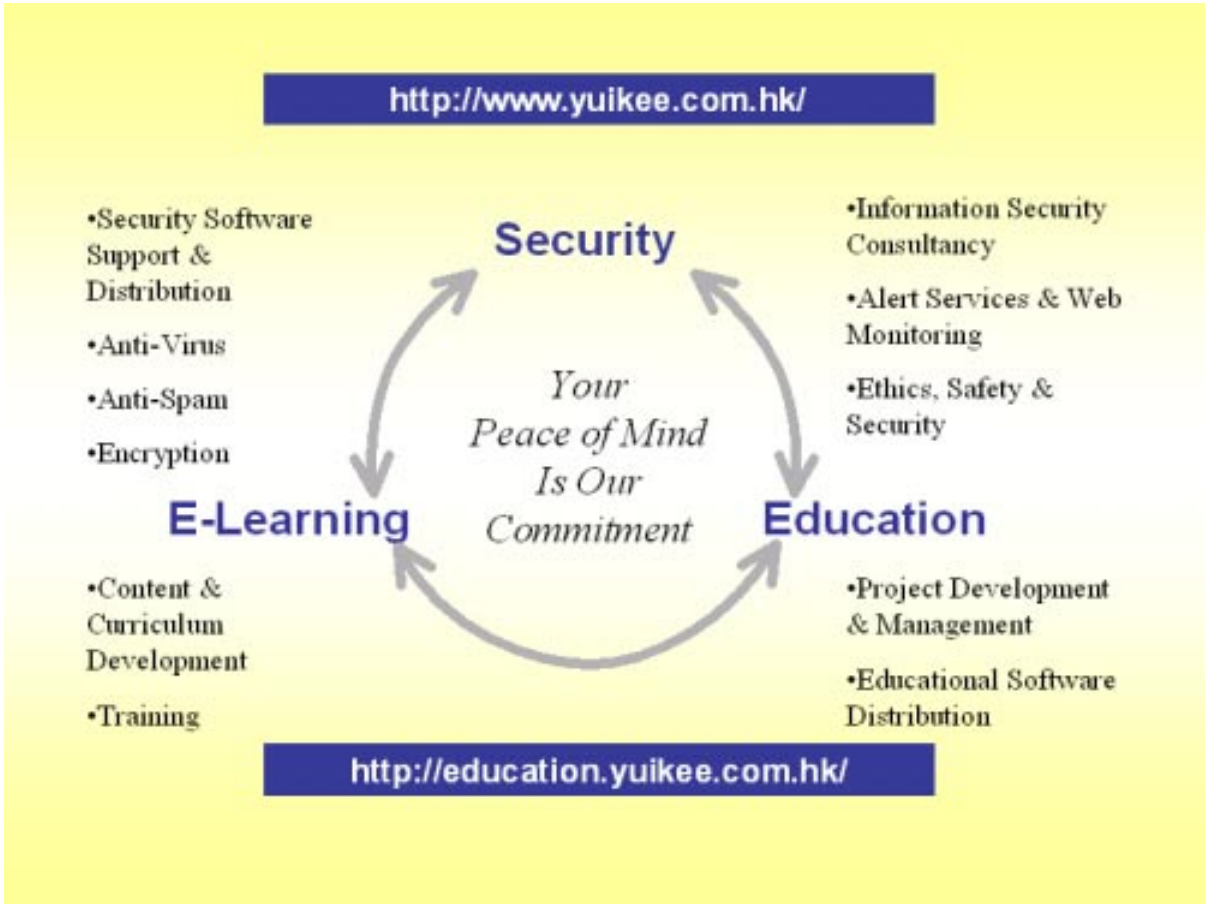
The following sftpg3 command would write checkpoints every 60 seconds and every 100 MB:

```
sftp> get --checksum=checkpoint --checkpoint=s60 --checkpoint=b100000000 largefile
```

One thing to remember when using checkpoints is that the file contents are not inspected when resuming the file transfer. The checkpoint keeps track of the location in the file, it does not notice if the file is changed after the transfer was interrupted. If there are other users or processes that might have modified the file between the file transfer interruption and restart, you should not use checkpoints. In that case, checksum can be set to md5 or sha1 to find a safe point where to resume the file transfer, but this consumes considerably more processing power than the checkpoints. If you have a process that is polling for the file to do further processing with it, you might want to use the 'prefix' option that uses a temporary filename with a prefix and removes the prefix part only when the transfer is ready.

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
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•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/