Yui Kee Computing Ltd.

Newsletter

April 2010

Contents

Protecting Your Identity Online

<web-link for this article>

Our occasional correspondent, Lirpa Loof, gives essential advice for protecting your identity online.

The online world has never been so dangerous, criminal gangs of phishers, botnet herds and lepidopterists roam websites and cyberspace, introducing bugs to trap the unwary. Protecting your money and information in these circumstances is difficult, but following a few, simple, rules will help:

Use your Password as your Pet's name

We all know that we should use long, complex passwords that are difficult to guess, but this makes them difficult to remember, too. What better way to remember your password than to use it for your treasured animal companion? When the creature finally dies, it is time to change your password. Use short-lived species for high security applications, such as online banking. Administrators who manage large numbers of systems may need a horde of mice, or, in extreme cases, an anthill.

Always Carry a Cheese-grater

We need to protect our security credentials from thieves and biometrics is becoming more popular. While giving a false password can gain you a little time when threatened, it is more difficult to fool an attacker with a fake biometric credential. A finger cast in silicone may fool a fingerprint reader, but is unlikely to satisfy a knife-wielding mugger. In these circumstances, a simple cheese-grater can be used to quickly and effectively erase the biometric credential.

Do Not Open Suspicious Emails

Just opening an email may expose you to dangerous malware. Suspicious emails may recognised by their innocuous subjects such as "urgent" or "Re: your document" and contents that, superficially, seem related to your work. Remember that the sender's address may be forged. For example, a message with the subject "urgent deadline!", supposedly from you boss

saying that a crucial report is due today is obviously a spear-phishing trap, and should be immediately deleted. Use your psychic powers to determine the contents of the messages before opening.

Following these rules will keep your important information safe, for the rest of the morning.

More Information

Trapping the unwary

PDF Specification Allows Arbitrary Execution

<web-link for this article>

Two security researchers, Jeremy Conway at NitroSecurity and Didier Stevens have demonstrated problems in the PDF specifications. Mr. Stevens has shown it is possible to embed malicious executables in PDFs and manipulate warning pop-up dialog boxes. A victim can therefore be tricked into running the malicious program. Mr. Conway has shown that Mr. Steven's technique can be used to create a PDF that will modify another PDF - potentially with a copy of itself, therefore making it a computer virus.

The problem affects any viewer following the PDF specification, it has been confirmed in both Adobe and FoxIT readers and those developers are working on mitigation. To be fair, the Adobe reader does present a warning that a file is about to be launched, but the text describing the file can be modified by the malicious PDF, allowing the user to be tricked into permitting the action. FoxIT simply launches the file without warning.

The PDF format was first created in 1993 as a portable document format, and has long been regarded as a "better" method of distributing documents because it is not platform-dependant. Other, perceived, advantages included ease of use, prevention of modification and inability to carry macro viruses. Some of these advantages are illusory, most users cannot modify PDF files because they use the free Adobe Reader application, which can only display and print, but not edit the files. The importance of the immunity to macro viruses faded when Microsoft introduced reasonable controls on their Office programming language. Conversely, the PDF file format was updated, eventually becoming the ISO 32000-1:2008 PDF open standard on July 1, 2008. The changes introduced included embedding arbitrary media types (e.g. songs and video), and execution of Javascript and external files, enabling the types of attacks described by Conway and Stevens.

More Information

Escape From PDF
Are PDF's Worm-able?
Worm-Able PDF Clarificaiton
Document management — Portable document format — Part 1: PDF 1.7
Does PDF stand for Problematic Document Format?
PDF security hole opens can of worms

More Secure Domain Name System Might Kill Connections on 5th May

<web-link for this article>

The 5th May 2010 is the date when the Internet's root domain name servers will change to using the DNSSEC protocol. The change adds digital signatures to DNS responses, making it more difficult for man-in-the-middle attacks to forge the responses and direct users to fake websites. In most cases, users will get the increased security completely transparently. However, the signatures increase the size of the UDP responses, and some internet systems

may block those packets because of their unusual size. This is particularly likely for firewalls, that treat UDP packets over 512 as damaged or malicious.

Keith Mitchell, head of engineering at root server operator Internet Systems Consortium, says his chief concern is large enterprises with sprawling networks. However many Small Office / Home Office devices may be affected too. Tests at Yui Kee have shown that at least one small router, the Linksys BEFXS41, will block large UDP packets when the Stateful Packet Inspection firewall option is turned on. While business-class firewalls will have configurable rules that can be edited to resolve the issue, consumer-class devices like the BEFSX41 usually have a simple "on/off" setting, leaving the user the choice between firewall protection or large UDP packets.

Administrators can easily check the DNS resolvers on their network either by using the Domain Name Systems Operations Analysis and Research Center's (DNS-ORAC) Reply Size Test Server or a Java tools from RIPE. Administrators should note that their clients may be using multiple recursive DNS resolvers, and the resolvers may be using multiple forwarders, and should therefore plan their tests to check all possibilities. If they find their resolvers have an issue, they can decide between:

- Solve the problem by modifying conflicting firewall rules.
- Solve the problem by replacing conflicting equipment.
- Mitigating the problem by configuring their resolvers to use a specific buffer size.
- Mitigating the problem by turning off options such as Stateful Packet Inspection on their equipment.

More Information

Will DNSSEC kill your internet?
OARC's DNS Reply Size Test Server
Testing your resolver for DNS reply size issues

The Power of Freedom of Information Requests

<web-link for this article>

A Gwent Police Officer is facing an investigation for gross misconduct after accidentally emailing a spreadsheet containing personal details of over ten thousand people to a journalist at online tech. publication The Register. The journalist's address was saved by the Officer's Novell email client after it was used for submission of two unrelated Freedom of Information requests last year. The autocomplete function inserted the address in the Cc field, instead of the address of the intended Police colleague when the Officer sent a file to Police officials. The file, which was not encrypted or password protected, contained 10,006 records of people applying for or in jobs that require a Criminal Records Bureau (CRB) check. *The Register* cooperated with Gwent Police in deleting the file, but declined to comply with their request not to publish a story reporting the incident.

The incident has been reported to the Independent Police Complaints Commission and the Information Commissioner, as required under the Data Protection Act. Investigators have exonerated the system design, and blamed human error. Yui Kee's Chief Consultant, Allan Dyer, commented, "While the officer concerned made a momentary addressing error, the fact that such a small mistake could have serious consequences indicates that there are system design improvements to be made." Some areas that could be considered are:

- **Autocomplete** This is a convenience feature in many email clients, but it often leads to addressing errors. This becomes more likely when the autocomplete allows partial entry of the name OR email address, as the possibility of multiple matches increases. A mistake becomes

harder to detect if the email client only displays the "friendly" name without the "technical" address, that contains the clue it is being sent to a different organisation than the one you expected.

- **Data Dissemination** Could the Officer have sent a link to where the data was stored? Why didn't the intended recipients of the data have access to the location it was stored in? It seems unlikely that five people could use over ten thousand records before they became outdated, so either live access to the original data, or a statistical summary of the data at a particular time is required; not a full copy with lack of timeliness and potential for mishandling.
- **Database Export** Why was it possible for so many records to be exported from the database by an ordinary user (unless the spreadsheet was the database, in which case the question is why was inappropriate software being used to manage the data)?
- **Protecting Confidentiality** Sensitive data should be covered by a policy requiring it to be encrypted in transit. Apart from the possibility of the file being erroneously sent out of the organisation, only a small number of Gwent Police Officers needed the information, so, given its sensitivity, shouldn't it be encrypted on the internal network?

More Information

Police send Reg hack CRB check database

Hong Kong Prepares to Relax Encryption Controls

<web-link for this article>

Hong Kong's Trade and Industry Department has gazetted an Order to amend amend Schedules 1 and 2 of the the Import and Export (Strategic Commodities) Regulations. The changes to Schedule 1 remove control of goods incorporating cryptography, but not having it as a primary function, or specifically produced for entertainment, mass commercial broadcast, DRM or medical records management. The changes to Schedule 2 remove information security products from the "more sensitive" group for strategic trade control, remove the license requirement for encryption devices in transit through Hong Kong, and allow encryption devices to be given license exemption under the Air Transshipment Cargo Exemption Scheme, if they fulfil all the terms and conditions of the Scheme.

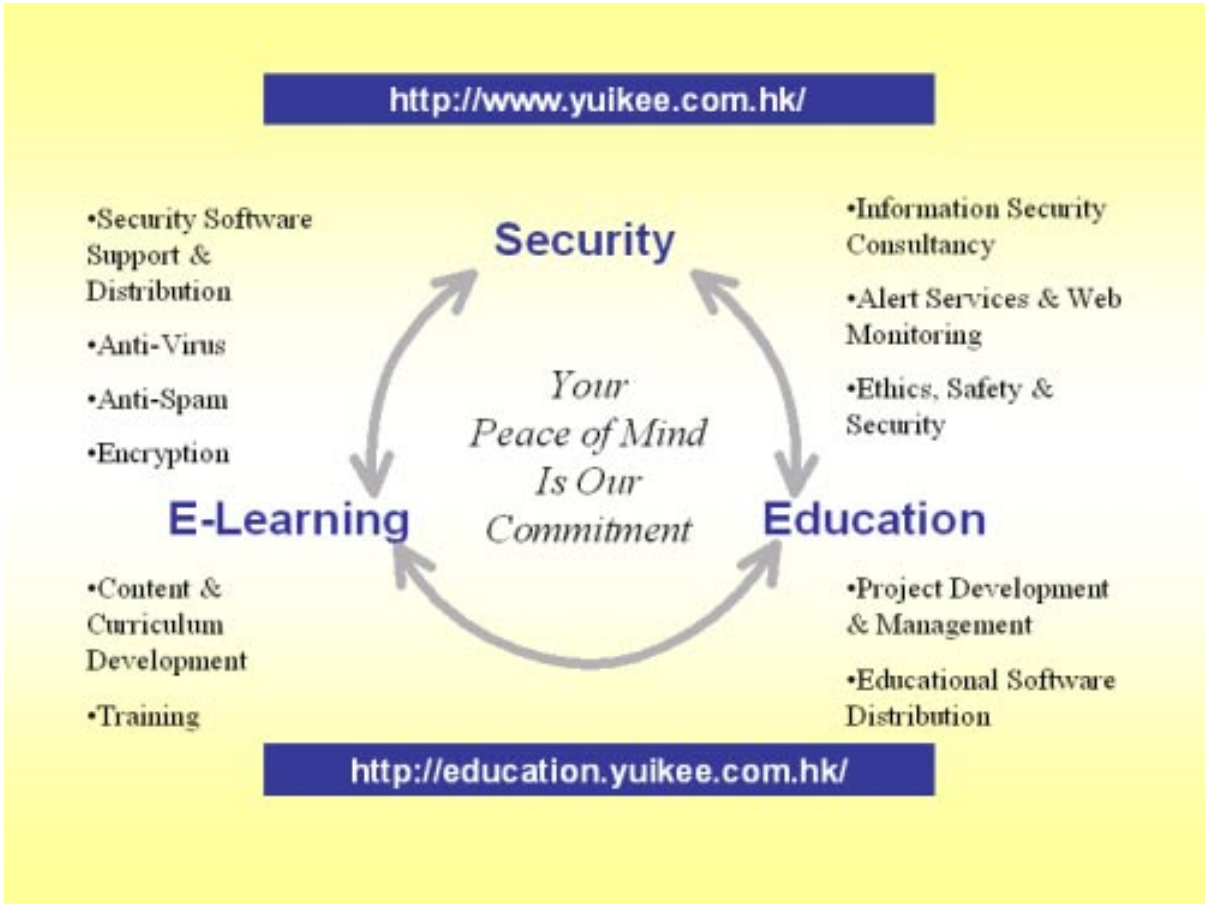
The Order will be tabled at the Legislative Council on 5 May 2010, and will come into effect as announced by the Director-General of Trade and Industry in a notice published in the Gazette.

More Information

Strategic Trade Controls Circular No. 2/2010 Amendment of Schedule 1 and 2 to the Import & Export (Strategic Commodities) Regulations

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/