Yui Kee Computing Ltd.

Newsletter

April 2007

Contents

Vista and Program Names

Vista will behave differently based on the *name* of an executable. If the name of a program contains "install", then it will automatically require Admin rights to run in Vista, unless it includes a Manifest. Other behaviour changes as well – Vista will prevent drag'n'drop of files into the program, and, if the GetVersionEx() function is used to test the OS version, Vista "lies" and reports Windows XP.

This appears to be a "feature" designed to improve compatibility with older installation programs, but it has generated considerable debate and could be seen as a security flaw.

More information:

http://www.theregister.com/2007/04/23/vista_program_naming_oddness/

http://www.theregister.com/2007/04/23/vista_program_naming_oddness/comments/#c_7221

Man-in-the-Middle Attack on Two Factor Authentication Online Banking

Four ABN Amro customers have been compensated by the bank for fraudulent withdrawals from their accounts. Criminals sent the victims forged emails, supposedly from the bank, with a trojan attached. The trojan redirected the victims to a fake bank website that requested their login details, including the temporary password from their security token. The information was used to concurrently login into the real bank website, and perform a withdrawal to the criminals' benefit.

However, the incident can be viewed differently:

- This isn't a failure of two factor authentication, like all phishing scams, it is a failure of the Bank to authenticate itself to the customer.
- PKI can deal with the man-in-the-middle. Essentially, the attacker is changing the message in transit, so a digitally–signed message would make modifications obvious.
- A general-purpose computer is unsuitable for secure transactions. We should build secure devices (PDA size) that are *only* used for signing. Download the document to be signed to the device (via USB, Bluetooth, etc...), read the document on the integral screen, plug

your token/smartcard holding your private key into the device, sign and upload. Any attempt to modify the device (hardware or software) breaks it.

But the bottom line is that criminals are highly motivated when stealing, and banks have a tendency to evaluate security solutions more on short-term costs and "user friendliness" than actually security.

More information:

http://www.computerweekly.com/Articles/2007/04/03/222857/abn-pays-out-over-hacked-accounts.htm

http://news.zdnet.co.uk/security/0,1000000189,39286766,00.htm

http://www.out-law.com/page-7967

Beware of Translation Software

Kingsoft Corporation, Beijing developer of Chinese–English translation software, caused problems for a Chinese furniture manufacturer by translating a colour description as “nigger brown” for a sofa shipped to Toronto, Canada.

More information:

http://www.theregister.com/2007/04/20/translation_error/

Long–Term Data Storage?

Scientists funded by the U.S. Department of Energy have demonstrated information storage by humans on bacterial genomes. Information storage on DNA is, of course, well–known … coding for the proteins required to build an organism is DNA’s function in living organisms. The large storage capacity and information replication abilities of DNA are also well–known. The scientists have demonstrated that it is possible to code arbitrary information (a short phrase) into DNA, and retrieve it later. This is not surprising, DNA synthesis is a well–known technique, and DNA sequencing is nowadays routine; both are currently used for genetic engineering experiments with far greater practical application.

Pak Wong, lead scientist on the project, suggested a scenario where “all critical information” could be coded on radiation–resistant bacteria, then, in the event of a devastating nuclear disaster, relief teams could retrieve the information from the bacteria on arrival. This does not address some important questions about the data retrieval:

i) Why didn’t the disaster recovery plan include storage of the critical information with the relief teams?

ii) If *all* other copies of the critical information were destroyed, where were the instructions on how to build a functioning DNA sequencer stored?

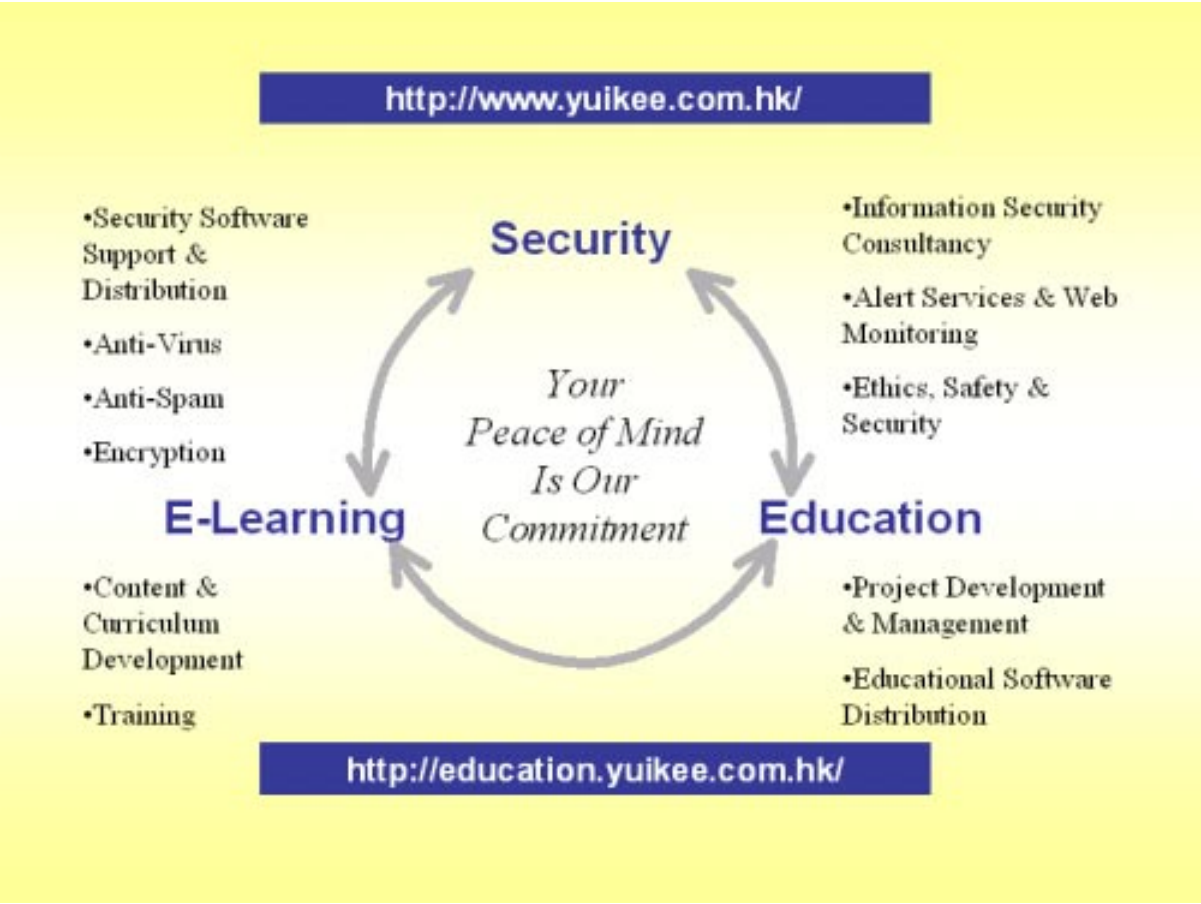
iii) Why would the intelligent descendants of cockroaches millions of years in the future have the slightest interest in the “critical information” stored on the bacteria?

More information:

http://www.cw.com.hk/computerworldhk/article/articleDetail.jsp?id=420180

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/
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/