Editorial: Information and computer security in the internet age

Eldon Y. Li

Department of Management Information Systems,
College of Commerce, National Chengchi University,
Taipei 11605, Taiwan
Fax: (+886)-2-2939-3754
E-mail: eli@calpoly.edu

Reference to this paper should be made as follows: Li, E.Y. (2007) 'Editorial: Information and computer security in the internet age', *Int. J. Information and Computer Security*, Vol. 1, No. 1/2, pp.1–4.

Biographical notes: Eldon Y. Li is the University Chair Professor of the Department of Management Information Systems at the National Chengchi University in Taiwan. He was the Professor and Dean of the College of Informatics at Yuan Ze University in Taiwan during 2003–2005. He served as a Professor and the Coordinator of the MIS Program at the College of Business, California Polytechnic State University, San Luis Obispo, California, USA, during 1982–2003. He visited the Department of Decision Sciences and Managerial Economics at the Chinese University of Hong Kong, during 1999–2000. He was the Professor and Founding Director of the Graduate Institute of Information Management at the National Chung Cheng University in Chia-Yi, Taiwan. He holds a PhD from Texas Tech University. His current research interests are in electronic business, human factors in Information Technology (IT), strategic IT planning, software engineering, quality assurance and information and systems management. He is the Series Editor of *Advances in Electronic Business*, published by Idea Group, USA. He also serves as the Editor-in-Chief of *Int. J. Electronic Business*, and four other related journals published by Inderscience, Switzerland. He is the Founding Executive Director of the International Consortium for Electronic Business (ICEB) and the former President of the Western Decision Sciences Institute (WDSI).

The information and computer security risk comes from many sources. Before the debut of personal computers, dumb terminals were used to access time-sharing systems. At that time, sending executable attachments with e-mail messages was impossible. All the security risk is confined in the central system. To break into a system, the hackers and attackers must access the computers and databases through the networked input devices in order to erase or overwrite programs or data stored in external storage media.

Historical perspective

Until IBM introduced the 8" floppy disk in 1971, stealing data or program was not easy because of the larger size of online media such as disk packs or tape reels. After Apple

Computers introduced Apple II Plus in 1979, computer viruses began to creep in. The first computer virus was found on Apple II's operating system in 1981. It spread widely through the pirated copies of video games. In IBM PC and compatibles, the first virus, 'Brain', emerged in 1986. The infection came through the boot sector of a floppy disk. To get infected, users must insert the floppy disk into the disk drive and actually read the disk. Therefore, the security risk could be easily managed in that era. However, with the advent of internet and WWW, the ball game has been entirely different. Besides reading an infected storage medium, users might get attacked by opening an attachment in an e-mail, clicking a hyperlink on a website or simply previewing an e-mail message in Microsoft Outlook. Even when they are not working or have turned off their computers, they might get too many spam messages and become unable to receive normal messages because of the disk quota overload; this is similar to 'denial of services' an ISP may encounter. The worst case is the invasion of spyware, which steals users' identities or critical information; the attack instructions of a spy agent that get downloaded on a victimised computer might vary based on the operating systems. Since the mid 1990s, the ubiquity of the internet has exacerbated the risk epidemic, enabling a virus to infect millions of people in a short period of time. For example in the year 2000, the 'Love Bug', also known as the 'I Love You' and 'LoveLetter' virus, spread from the Phillipines over to the US and Europe. In only 6 hours, it infected 2.5 million PCs causing an estimated US$8.7 billion in damage. Other infamous viruses include 'Klez .H' (US$13.9 billion) and 'Sobig' (US$29.7 billion) that were extremely prolific in 2003.

Preparing for the unthinkables

In the internet era, the security risk of an organisation may come in any form, at any time, and from any place. It is a jungle out there; we must prepare for the unthinkables. Unthinkables such as the 11th September attack and more recently the hurricane Katrina in the U.S., tell us that organisations must stay resilient and get ready for disaster recovery at any time. Deutsche Bank in Germany, as an example, was able to activate its backup systems in Ireland and went on to clear more than $300 billion in transactions on the same day when the South Tower of the World Trade Center collapsed on its New York facility. However, this seems to be the exception rather than the norm. A recent survey in 2005 by nCircle Network Security, Inc. of San Francisco (see http://www.ncircle.com /index.php?s=news_press_2005_0711) polled 1,700 CIOs, CSOs and Security Directors and reveals that many businesses still lack the information about the effectiveness of their security systems. The results indicate that 60% of the respondents were unable to determine the trend of their network security risk. More than half (58%) of them stated that they are unable to generate reports about applications or vulnerabilities on their network by region, business unit or business owner. Furthermore, 52% of them stated that they have no way to verify and manage compliance with their own internal security policies. The results of this survey call for two needed-services: education and disaster-recovery services. For education service, the academic institutions should answer this call and include a core course of information and computer risk management for all students in the curriculum and other various related elective courses for computer science or information systems students in particular. Regarding the disaster-recovery service, the industry should answer the call and make it more affordable for small and medium enterprises to use the service.

User beware

Today's hackers could not only send viruses or worms to users directly via e-mail messages, but they could also enter into a web server to change the code of a hyperlink so that when a user clicks on the hyperlink, a malice program is downloaded and executed. To protect from attack, end users must be beware of the possible sources of viruses and worms. The following suggestions might help.

- Install anti-virus software and activate its online virus protection function.
- Do not execute program code from unknown sources. Do not allow your web browser to execute Active-X code without your consent.
- Turn on your firewall to protect from eavesdropping of hackers.
- Create user account and password for your PC, to protect from local or remote access by hackers.
- Do not preview an e-mail message from unknown source. Use junk control function to mark it as junk and delete it without previewing it.
- Do not download attachment file without file extension, or with such file extension as PIF, WMF, EXE, BAT, INI. The first four types of files are executable, while INI could change your software or hardware configuration.
- Before clicking on a hyperlink, review its URL to know where you are going. Do not go to an unknown site.
- Finally, turn off your computer when you are not online.

The call for actions

As computer users in a corporate office, we urge the ICT industries to take a more active role in defending us. They should engage and fight the hackers and cyber-terrorists at the network entrance, using not only software but also hardware to prevent their malice code from entering into users' network and computer systems. For example, communication's hardware manufacturers are embedding firewalls and anti-virus filters in their network routers. Microsoft is introducing Vista operating systems to provide better security for PCs. With the aforementioned calls in mind, the aim of *International Journal of Information and Computer Security* (IJICS) is to promote and coordinate developments of information and computer security in the fields of information technology, political science, informatics, sociology, engineering and science. It focuses on theory, design, implementation, analysis and application of secure information and computer systems. The Journal publishes original and review papers, technical reports, case studies, conference reports, management reports, book reviews, notes and commentaries, as well as emerging issues of interest to professionals and academicians. We invite articles representing synergy between academic and business as well as theory and practices.

Finally, we express our gratitude to Inderscience's staff for their high-quality professional assistance during the pre-publication process and to our editorial team and board members for their continuous support during the journal's planning phase. Our

most sincere thanks go to all the authors who share their knowledge and research outcomes with the readers of this inaugural issue. Without them, the debut of this journal would not be possible. Finally, we thank our readers around the world, for using this journal as a source of information and hope you find it helpful in your research endeavours.