Information Systems Security, 16:195–202, 2007

ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701576412

Taylor & Francis
Taylor & Francis Group

Awareness Education as the Key to Ransomware Prevention

Xin Luo
School of Business,
Virginia State University,
Petersburg, VA, USA

Qinyu Liao
School of Business,
The University of Texas
at Brownsville and
Texas Southmost College,
Brownsville, TX, USA

Address correspondence to
Xin Luo,
Department of Computer Information Systems, School of Business,
Virginia State University,
Petersburg, Virginia, 23806.
E-mail: xluo@vsu.edu

INTRODUCTION AND BACKGROUND

In the paradigm of Information Systems (IS), information security research has received increased attention from both academic researchers and industry practitioners alike. This intriguing phenomena is related to the growing recognition that, notwithstanding the advances in information technology (IT) for data collection, storage, and processing at a remarkable rate, users' concerns over security of what is surreptitiously collected and the privacy violations resulting from their misuse of IT have also skyrocketed. Such sophisticated threats as phishing, pharming, and spyware have further exacerbated users' worries about information confidentiality, integrity, and availability. Therefore, understanding of pertinent issues in information security vis-à-vis technical, theoretical, managerial, and regulatory aspects of information systems is becoming increasingly important to the IT community.

Today's organizations confront not only keen peer competition in business society but also increasingly sophisticated information security threats in cyber world, as online presence and business transaction are considered as a possible profit-driven avenue and a necessary means for global competence. In computer virology, as technologies continue to evolve, advanced encryption algorithms, on the positive side, can be utilized to effectively protect valuable information assets of enterprises. On the negative side, however, they can also be employed by malicious attackers to conduct pernicious activities in search of profits or benefits. Past information security research has investigated such malware programs as Trojan horse, worms, and spyware from a plethora of scientific perspectives (Warkentin, Luo, and Templeton, 2005), and relevant strategies and tactics have been proposed to alleviate and eradicate the cyber threats (Luo, 2006).

Recently, the emergence of a new form of malware in cyberspace known as ransomware or cryptovirus has drawn attention among information security practitioners and researchers. Imposing serious threats to information assets protection, ransomware victimizes Internet users by hijacking user files, encrypting them, and then demanding payment in exchange for the decryption key. Seeking system vulnerabilities, ransomeware invariably tries to seize control over the victim's files or computer until the victim agrees to the attacker's demands, usually by transferring funds to the designated online currency accounts such as eGold or Webmoney or by purchasing

a certain amount of pharmaceutical drugs from the attacker's designated online pharmacy stores.

This article is the first attempt to address ransomware in information systems security research. In an effort to cater to both security practitioners and researchers, the rest of this article is organized by four parts. Part 1 addresses ransomware's underpinning structures; recent statistics and attack methodologies of ransomware infection are also presented. Part 2 compares the technological differences between ransomeware and Trojan horse, worm, and spyware; a sample attack scheme is listed to address the attacking process. Part 3 discusses the future trend of ransomware in terms of technological sophistication level, and part 4 proposes a model of ransomeware prevention and relevant recommendations for ransomware prevention are presented.

TECHNOLOGICAL INVESTIGATION OF RANSOMWARE

In the cyber world, computer users have faced certain types of threat such as worms, spyware, phishing, viruses, and other malware. Ransomeware is an extortion scheme whereby attackers hijack and encrypt the victim's computer files and then demand a ransom from the victim for these files in original condition. We thereby define ransomware as a piece of pernicious software that exploits a user's computer vulnerabilities to sneak into the victim's computer and encrypt his or her files; then the attacker keeps the files locked unless the victim agrees to pay a ransom. In a typical ransomware attack, the attacker reaches into a compromised computer by seeking the exposed system vulnerabilities. If this system was victimized earlier by a worm or Trojan, the attacker can easily enter the weakly configured system. He then searches for various types of important files with such extension names as *.txt, .doc, .rft, .ppt, .chm, .cpp, .asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, .jpg, .key, .mdb, .pgp .pdf.* Knowing these files are of possible crucial importance to the victims, he then encrypts these files, making them impossible for the victim or owner to access them. Later, the attacker sends the victim an email ransom or pop-up window demanding for the encryption key that unlocks the frozen files.

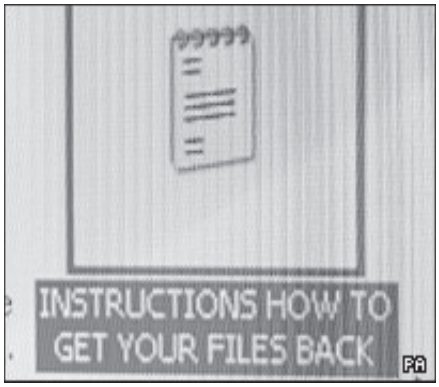

FIGURE 1 **Notification of Hijacked Files**

Once the attacker locates these files, there are several processing strategies he might implement. First, he can compress all the located files into a password-protected zip package, then remove the original files; second, he can individually encrypt each located file and then remove the original files. For example, if the original file is "*DissertationFinalVersion.doc*", ransomware will create a file such as "*Encrypted_DissertationFinalVersion.doc*" in order to label the original file; third, the attacker might create a hidden folder and move all the located files to this folder, producing a pseudophase to deceive the victim. The third strategy, of course, carries the slightest damage and is comparatively feasible for victim to retrieve all the "lost" files.

Furthermore, when ransomware attacks successfully take control of an enterprise's data, the attacker encrypts the data using sophisticated algorithm. The password to the encryption is only released if ransom is paid to the attackers carrying out the attack. The attacker usually notifies the victim by means of a striking message (Figure 1), which carries specific instructions as to how the victim reacts to retrieve the lost files. A text file (Figure 2) or pop-up window message is generally created in the same folder where files are encrypted. The text file or message box clearly indicates that all the important files are already encrypted and informs the victim of specific money remittance methods. A ransomware message example in the short form could look like this:

- Pay $10.99 via Western Union otherwise you will keep getting this screen.
- One file per 30 minutes will be deleted from the hard drive. Deleted files will be restored when you have paid up and entered the proper unlock code.

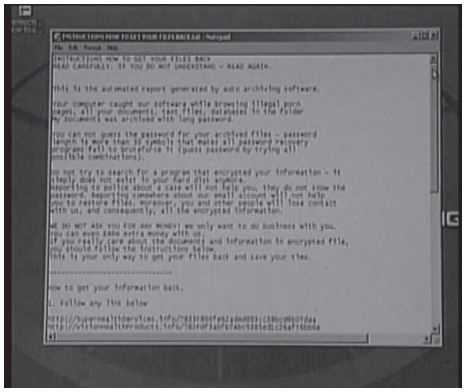

FIGURE 2 **Text Ransom Note**

- Antivirus software can not detect this virus, nor can it detect the hidden folders in which the deleted files are stored.
- When entering a false unlock code, there is also a message stating that the hard drive will crash in three days.

Figure 3 shows in Chinese a pop-up window telling users how to deliver ransom to get files back. Information includes the amount of ransom required, the account number for depositing the ransom money, a cell phone number for deposit notification, and the method to recover the file with a given unlock code after the money is sent.

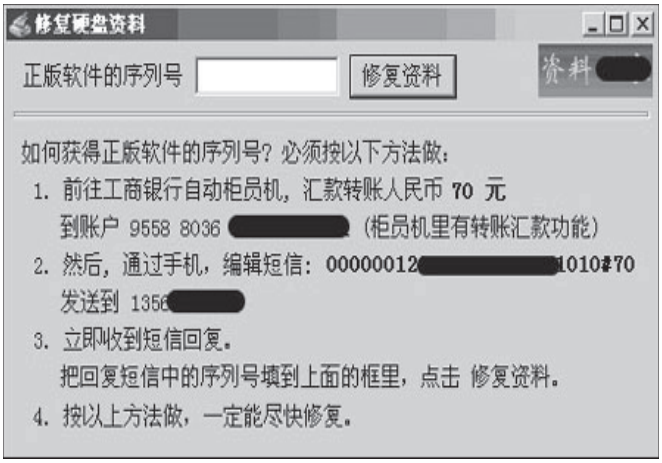

FIGURE 3 **Pop-up Window for Ransom Delivery Instructions in Chinese**

Table 1 lists all the methodologies used by recent ransomware attacks and ransom methodologies as to what attacker demands for.

THEORETICAL COMPARISONS OF RANSOMWARE VS. OTHERS

Ransomwares are induced through Internet like other computer virus such as Trojan horse, worms, and spyware. This part compares ransomware

TABLE 1 **Typical ransomware attack and function methodologies**

Name	Time	Attack Methodologies	Ransom Methodologies
Trojan.Pluder.a	6/14/2006	Copy different types of file to hidden folders	Remit $10 to designated Chinese Industrial and Commercial Bank
Arhiveus	5/5/2006	Link all the files in folder "My Documents" to a single file named EncryptedFiles.als, and delete all the original files. Create a text file named "INSTRUCTIONS HOW TO GET YOUR FILES BACK.txt" in the folder, directing how users can receive the decrypt key, which exists in the malicious codes	Ask victims to purchase $75 pharmaceutical products from certain Russian websites. Once victims make the purchase and email the order ID to the attacker, the ID will be confirmed by the attacker, who will email the decryption key back to the victims if the ID is validated.
Trojan.Randsom.A	5/1/2006	A notification window always shows above other windows to distract victims. This bluffs that a file is deleted every 30 minutes, but no files are indeed deleted	Remit $10.99 through Western Union
Trojan.Cryzip Trojan.Cryzip Variant	3/11/2006 3/22/2006	Compress document files (txt, doc, rft, etc.), database files, and multimedia files into a password-protected ZIP file. The decryption key used for the ZIP file is stored in file Cryzip. The decryption key can be dynamically downloaded for Cryzip's new version	Notify victims to remit $300 to a designated E-Gold account. Specific instructions are given.
Trojan.PGPCode	5/23/2005	Encrypts all files using RSA algorithm	Notify victims to remit $200 to a designated E-Gold account.

with other types of malware from a technological perspective.

Unlike viruses, Trojan horse virus is a type of virus that doesn't replicate itself. Trojans get into a computer by hiding inside other software, such as an email attachment or download. They are destructive programs that masquerade as benign applications. One of the most insidious types of Trojan horse is a program that claims to rid the user's computer of viruses but instead introduces viruses onto his or her computer.

Worms, on the other hand, are the most prevalent type of virus that can spread themselves, not just from file to file but from computer to computer via email and other Internet traffic. Worms find the email address book of the intruded computer and help themselves to the addresses and send themselves to all the contacts, using the victim's email addresses as the return address.

Spyware, defined as a client-side software component that monitors the use of client activity and sends the collected data to a remote machine, surreptitiously comes hidden in free downloadable software and tracks, or uses movements, mines the information stored on victims' computer, or use the computers' CPU and storage for some tasks the victims know nothing about. The information collection by the spyware can be going on when the victims are not even on the Web and can stay on victims' computers long after they've uninstalled the original software.

Unlike worms, ransomware is not able to actively propagate for wide infections. Therefore, security professionals could obtain sample infection code and further analyze it for possible solutions. Similar to Trojan horses, most ransomware infections stem from victim's lack of attention on unknown email attachment, careless browsing and download from malware-embedded Web pages that exploits security flaws in a browser. Thus we believe that ransomware is the second-generation malicious software that deploys attacking strategies seeking system vulnerabilities potentially caused by its precedents. As aforementioned, a typical ransomware attack seeks targets that are victimized earlier by a worm or Trojan and then grabs a slew of files. The attacker employs a cryptosystem to encrypt those files, and then sends the victim a notification which normally emphasizes that:

1. The files are encrypted and other decryption or anti-virus software won't work;
2. Following the instruction in the notification is the only solution;
3. Reporting to law enforcement or relevant bureaus cannot resolve this problem; and
4. Timely remittance is required; otherwise files will be removed.

Ransome viruses can be spread in several ways, including through spam or a so-called drive-by download that exploits a browser's vulnerability when a user visits a malicious Web site. Figure 4 lists a ransomware extortion schema, which indicates the process where ransomware penetrates the system, encrypts important user files, and demand for ransom. The earliest ransomware simply stored the kidnapped files in compressed archives, then password-protected those archives. In 2006, however, attackers turned to asymmetric encryption, like RSA, to lock hijacked data.

NEW DEVELOPMENT IN RANSOMWARE: WHAT IS ON THE WAY?

The emergence of a new form of ransomware is an example of criminal moving faster than the technology security. It is argued that we will probably get to the point where we are not able to reverse the encryption, as the length of ransomware encryption keys are pushing the boundaries of modern cryptography. For example, if we add a rootkit to hide the installer of the ransomware so that if we break its password it then randomly encrypts the files again, or after say five failed logins it scrambles everything. In this way it can hold us to total ransom. But so far no fancy rootkits like this have been reported. Overall, Trojans that archive data tend to present a threat to Western users; Russian virus writers are more likely to use data encryption for blackmail purposes.

Despite the keen efforts that enterprises have contributed toward information security hardening, we deem that the occurrences of ransomware will continue to rise. More important, the encryption algorithms used by ransomware writers will become increasingly complicated. As more technologically

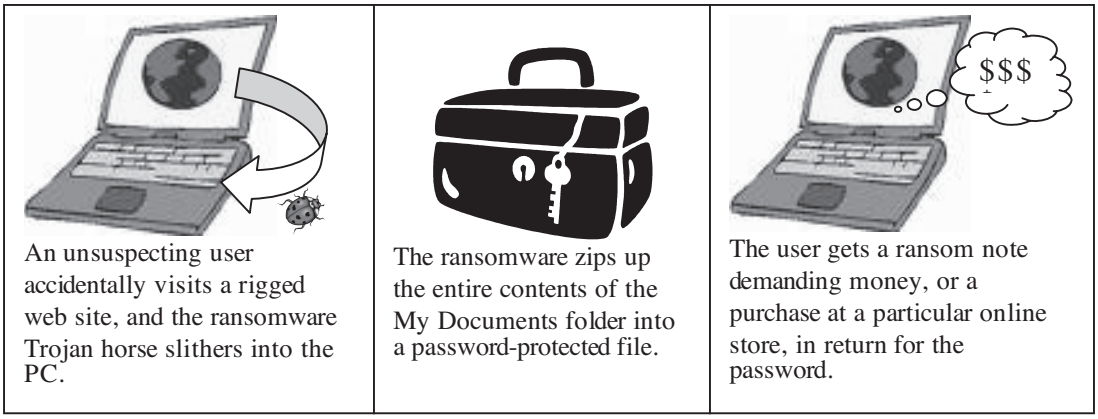

FIGURE 4 **Ransomwares Extortion Scheme Adapted from Brant (2006)**

sophisticated encryption technologies are employed for cyber crime, an encryption war between the malicious perpetrators and the security professionals seems inevitable and increasingly intense. This scenario, again, mirrors what we have witnessed in a cat-and-mouse battle between virus producers and antivirus companies in computer virology. As such, security professionals endeavor to crack the encrypted code, and attackers, in turn, promptly respond back with more complex methodologies. By the same token, simple encryption codes being cracked by security professionals will trigger the birth of further complicated encryption seeking ransom. Recently, complex incarnations RSA encryption embarks and ransomware writers will continue to seek for increasingly sophisticated methods of password-protecting and hiding corrupted files.

Social engineering is now also involved in the spreading of ransomware, as the attackers tend to exploit such popular Websites as online recruitment to victimize unwary users. Furthermore, RSA algorithm or any other similar algorithm which uses a public key will continue to generate far more complicated digital keys in terms of bit unit. The initial 50-bit key which did not pose any difficulties for security professionals has enabled attackers to rethink the attacking approach and to birth 260-bit key, which has been extended to a 330-bit key. In addition, the recent emergence of Gpcode ransom virus featured a 660-bit key, which could take security professionals about 30 years to break using a 2.2 GHz computer.

Based on Kaspersky's research, it is argued that the encryption methods are reaching the limits of modern cryptography. As such, future incarnations could be theoretically unbreakable, thereby forcing the IT community to face a dilemma in that those infected may have no choice but unwillingly to pay the ransoms in order to unlock their important files. Even though the documented ransomware attacks have been rare, the use of asymmetric encryption in malicious programs may continue to evolve to exploit computer user for the gain of profit. According to Alexander Gostev, a senior virus analyst, it's only a matter of time before ransomware hackers have the upper hand. As the criminals turn to ever-more-elaborate encryption, they may be able to outpace and outwit antivirus vendor researchers. With a longer key that could appear at any time in a new creation, information security businesses may fail to win the war, even if maximum computing power were to be applied to decrypting the key. Ransomware will undoubtedly remain a major headache for the security industry. Figure 5 categorizes different types of ransomware, based on the degree to which threat severity varies.

STRATEGIC RECOMMENDATIONS FOR ANTI-RANSOMWARE

Ransomware started off in the business community and has now extended more into the consumer space because, while businesses regularly back-up data and follow set security policies, at-home and small business users usually neglect both. What is maddening about ransomware is the way it steals personal information by using a technology that is also the backbone of Internet users' security. It will undoubtedly remain a major headache for the

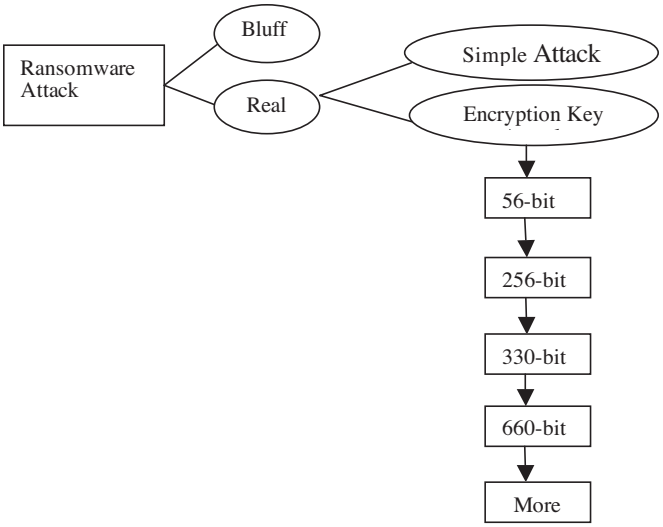

FIGURE 5 **Ransomware Categorization on Threat Severity**

antivirus industry, at least in the near future (Oswald 2006).

Due to the extensive use of the internet and the nature of ransomware, this article proposes a four-step framework (Figure 6) for proactive prevention of ransomware threat. The key is to promote the awareness education of corporate employees, management as well as individuals users and small business owners.

Policy/procedure/regulation

As more businesses depend on IT to enhance business operation efficiency and stay competitive in the market, the security of company and customer information becomes an important issue relating to business performance and success. Although ransomware is being viewed primarily as a threat to individuals and home computers at the moment (Mueller, 2006), because most companies have devices at the perimeter that constantly monitor for malicious activity and take steps when signs of malicious activity occur. However, many companies did experience losing critical business data and even system failure, trigged by other forms of malware. Companies are deluding themselves if they think ransomeware is just for home users.

An informative procedure to regulate ransomware should be included in the general information security and privacy policy to minimize ransomware occurrence. They should ask themselves questions such as

- Do we have any experience in detecting ransomware attacks?
- Can we offer protection against security attacks that occur quickly?
- If our company comes under a ransomware attack, how might we be able to help end users quickly decrypt the affected files?
- Once a vulnerability is found, how long do we typically take to distribute a patch?
- If I suspect a thwarted ransomware attach, how should I report, and how will I inform the authorities while protecting my confidential information?
- What kind of innovative technology do we offer to battle dangers such as Trojan horse and key loggers that work through the Web and often go undetected by antivirus software?

A good policy with procedure is the first step in protecting corporate from ransomware threat. It provides a guideline for inexperienced users. However, management level support is needed for policy and procedure enforcement.

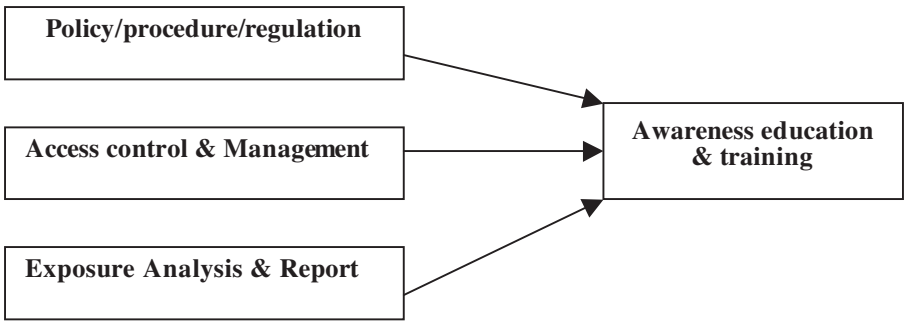

FIGURE 6 **Framework for Ransomware Prevention**

Access Control and Management

Ransomware is currently a PC problem, not a Mac problem The good news in ransomware prevention is you don't need special ransomware procedures to protect yourself or your computer network from ransomware. The multiple layers of security that the typical corporation already has in place will most likely stop the ransonware before it infects the network, because ransomware needs to first seek system vulnerabilities prior to its breach (Fontana, 2005). The same methods of protection can be recommended for small business and home users: Use firewalls that control what information people can access on your computer; have up-to-date antivirus and anti-spyware software; keep your browser, system software, and other software up-to-date with the latest security patches; use a pop-up blocker if you don't already have one because much ransomware is delivered via pop-ups to keep the computer from being compromised in the first place; be careful about downloading software—games, screensavers, etc., and never accept downloads from unknown Websites or pop-up windows; avoid opening unfamiliar email attachments and prohibit P2P file sharing and downloading; and back up your own personal computer files and system files and important emails regularly onto movable media.

The access control and management can be achieved by a centralized IT structure where multilayer prevention solutions can be efficiently managed by IT professionals for maintenance, troubleshooting, and compliance management. It is important that IT professionals are given the authority to enforce the ransomware prevention policy to prohibit potential risks and damages.

Exposure Analysis and Report

A report system, either via internal email or enterprise instant messaging, should be used to regularly make users aware of the system patches or updates to protect their computers. In turn, users should follow the instructions of the report. In addition to system hardening, we suggest that if people find themselves being blackmailed, they should contact their local law enforcement instead of simply remitting money to the attacker. They should also contact their network security management and software security vendor who might be able to provide possible technical supporting by recovering their work. This would provide security professionals with attacking traces for possible solutions.

Although ransomware incidents have shown a sharp rise, it is not as profitable as other types of online financial fraud because most of the people affected are small businesses and home users who failed to follow the file backup and security procedures. Due to the unorganized and on-off nature, there is also a lack of law enforcement to deal properly with ransomware incidents. In the United States, ransomware cases would previously have been dealt with by the National High Tech Crime Unit, which was amalgamated into the Serious and Organized Crime Agency (SOCA) in April 2006. It falls out of SOCA's remit. E-crime is a concern of SOCA, but it cannot investigate on individual petty theft cases. Therefore, it is important for ransomware victims to expose the incidents and report their losses. Widespread public outcry can draw the attention of the legislators for legislative actions against ransomware.

Awareness Education and Training

Ransomware threatens to dissuade people from participating in ecommerce. The computer, banking, and retail industries need to develop and implement a major initiative to educate current and potential customers on how to be safe and secure online.

Currently, there is no panacea to the eradication of ransomware. Companies should take steps to raise employee awareness, from altering employees about new threats and existing policies and procedures, to brown bag luncheons and asking employees to sign documents attesting to their security and confidentiality standards. The key is to show employees how ransomware induced by a security lap can directly impact them and their company. For example, the company could lose stock value or important customers. The company could be shut down. When people understand how their behavior can affect their customers, their company, or themselves, they are more likely to take steps to protect themselves and comply with the policy, procedure, and regulations.

CONCLUSION

With occurrences of ransomware on the rise, the encryption algorithms employed are becoming increasingly sophisticated. Ransomware will undoubtedly continue to be a serious challenge for both information security professionals and researchers, as future incarnations could be unbreakable and the encryption methods, powered by social engineering, are reaching the limits of modern cryptography. Enterprises and individual users should take preventative measures to regularly back up important data and continuously harden their systems from different layers. The proposed framework involves four steps in ransomware prevention. The key is to proactively deter ransomware attacks through awareness at the management, IT, and end-user level. We hope this framework can guide organizations to more effectively cope with the increasingly sophisticated threats of ransomware.

BIOGRAPHY

Dr. Xin Luo is an Assistant Professor of Computer Information Systems in School of Business at Virginia State University, USA. He received his Ph.D. in Information Systems from Mississippi State University. He has an undergraduate degree in International Business from Sichuan Normal University, China, an MBA from The University of Louisiana, and an MSIS in Information Systems from Mississippi State University. His research interests center around information security, E-commerce/M-commerce, and global IT adoption and management. He is the Managing Editor of *Journal of Internet Banking and Commerce*. He has published numerous research papers and attended international & national conferences including *Communications of the ACM, Information Systems Security, International Journal of Information Security and Privacy, Journal of Internet Banking and Commerce, AMCIS, DSI,* and *IRMA* etc.

Dr. Qinyu Liao is an Assistant Professor of Management Information Systems at the University of Texas at Brownsville. She got her PhD in Business Information Systems from Mississippi State University. Her research interests are in electronic commerce, computer security, information systems in education and end user behavior and adoption. She has published articles in the *Journal of Internet Banking and Commerce,* and in conferences proceedings including Americas Conference on Information Systems, the Southwest Decision Science Institute Conference, International Conference of Management Science and Application, Global Conference on Business and Finance, among others.

References

Brant, A. (2006). "The 10 Biggest Security Risks You Don't Know About." *PC World,* 76-88.

Fontana, J. (2005). "The Service-Oriented Business App." *Buzz Issues,* 96-97.

Luo, X. (2006). "A Holistic Approach for Managing Spyware." *Information Systems Security,* 15: 2, May-June

Mueller, L. (2006). Webjacking, and how to boot it out. *Network Security,* Vol. 2006, Issue 6, p. 15-18.

Oswald, E. (2006). Ransomware Becoming a Serious Problem. *BetaNews,* July 24, 2006. Retrieved October 25, 2006, from http://www.betanews.com/article/Ransomware_Becoming_a_Serious_Problem/1153780370

Warkentin, M., Luo, X., and Templeton, G. F. (2005). "A Framework for Spyware Assessment," *Communications of the ACM,* 48: 8, pp. 79-84.