E-Literacy in Pacific Asia

Nena Lim[1], Colin Ferguson[2]
[1]limn@unimelb.edu.au [2]colinf@unimelb.edu.au
Department of Accounting and Business Information Systems
The University of Melbourne, Melbourne, VIC 3010, Australia

Abstract: Hesitant about Internet security has been a major obstacle to consumers' acceptance of electronic commerce. The objective of this paper is to assess how consumers in Pacific Asia perceive Internet security and how much they know about the topic. A total of 182 university students from Australia and Hong Kong SAR participated in this study. The results show that respondents in these two Pacific Asia regions had similar level of e-literacy. Both groups were unsure about Internet security and their self-assessed knowledge of Internet security was relatively low. A closer analysis of the data suggests that respondents have a tendency to over-estimate their understanding of the Internet security.

Keywords: Internet security and privacy, e-literacy.

I. Introduction

The rapid growth and influence of the Internet is increasingly pervasive in our everyday life. Businesses make use of the Internet to facilitate marketing, training, as well as improve their relationships with their suppliers and customers. Despite an increasing number of consumers who adopt electronic commerce, the overall adoption rate of electronic commerce has so far been below expectation [1]. As a result, much research tries to investigate what motivates consumers to purchase products or services online [2] [28]. For example, [35] examine choice and convenience issues. Interestingly, although security was considered to be a building block for electronic commerce growth [29] and hesitant about Internet security has been found to be a major obstacle to consumers' acceptance of electronic commerce [17] [27] [30] [31] [38] [40], most Internet security research focuses on developing more advanced and sophisticated Internet security measures [25] [36] [37] and assume consumers are knowledgeable about the topic [10].

Little research to date has examined how much consumers know about or understand Internet security. The importance of educating company staff electronic commerce (e-commerce) knowledge was emphasized in [34]. Researchers have proposed to investigate individuals' knowledge of security threats and countermeasures [7]. In another study, 275 undergraduate students from three different states in the United States were asked how they perceived Internet security and whether they knew any of the security control techniques used by business [17]. The results show that 80% of respondents believed that Internet vendors use security control measures to protect customers. In addition, nearly 70% of respondents had heard of encryption, about 50% had heard of secure electronic transaction (SET), but only one-fourth had heard of secure socket layer (SSL). Nonetheless, hearing about certain security techniques equals neither understanding nor trusting of those security techniques.

Many consumers worldwide are attracted to use the Internet especially the WWW because of its friendly graphical user interface. Nevertheless, the majority does not know what security measures are used by businesses, how the measures work to enhance Internet security, and what limitations the measures have. Even experienced computer users or Internet users are likely to have only limited knowledge on Internet security. The problem is, without a reasonable level of knowledge of Internet security such as digital certificates, it means that security can be easily compromised because of the ignorance of users [36]. If a consumer is confronted with a warning regarding suspicious server digital certificate while accessing a Web-site, it is unlikely he/she understands what it means or knows what to do [16]. The objective of this study is to assess how consumers in Pacific Asia perceive Internet security and how much they know about the topic.

The rest of this paper proceeds as follows. Section 2 briefly describes the different components of Internet security. Section 3 describes the research methodology. Section 4 describes the technology adoption situations in Australia and Hong Kong SAR. Section 5 presents the research results. Finally, the paper is concluded in section 6.

II. Internet Security

As the Internet is boundless, how can one party be sure the identity of the other party in an Internet transaction and ensure information can be exchanged in a secure manner? One of the strategies businesses use to tackle this problem is the adoption of digital certificates (also known as electronic certificates) for Internet communications and transactions [3] [33]. Each digital certificate includes information such as the name of the certificate holder/organization, a unique serial number, the expiration date of the certificate, a copy of the certificate holder/organization's public key, and a digital signature of the certification authority. The objective of digital certificate is to verify the identity of an individual or organization in the cyber world. It is similar to real world how individuals use passports to identify themselves. The importance of digital certificates should not be

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 452 - 456.

underestimated. An incident in 2001 which involved Verisign issued two certificates mistakenly as Microsoft staff has caused Microsoft Corporation to issue a major update of its software [8] [19].

The mechanism of digital certificates relies on a public key infrastructure (PKI) to achieve on-line authentication [8]. Based on a model of trust [12], a PKI is a system for issuing, distributing and using public keys used in public key cryptography [24] [37]. It comprises digital certificates, certificate authorities and key repositories, etc. [12] [24]. The underlying mechanism of a PKI relies on public key cryptography which was developed in 1970s [21] [24]. Public key cryptography involves two mathematically related keys - private and public keys. Private and public key pairs are issued by trusted third parties called certification authorities (CA) [39]. Under a PKI, individuals with no prior relationship can achieve confidentiality and authentication when they swap information over the Internet or conduct electronic commerce transactions [21]. As a result of a PKI system, individuals and organizations can digitally sign and encrypt email messages. Moreover, two parties, typically a business Web sever and a consumer, can set up a secure socket layer session to exchange information safely [26].

III. Research Methodology

To examine the research questions, we conducted a Likert-scale style survey. We chose samples from Australia and Hong Kong SAR because these two regions were ranked the highest in Pacific Asia in Economist Intelligence Unit (EIU)'s annual report on e-readiness in 2003. In that report, Australia ranked the 9th and Hong Kong SAR ranked the 10th (tied with Canada) [18]. Two Scandinavian countries, Sweden and Denmark, were ranked number one and two on EIU's 2003 e-readiness ranking. E-readiness measures a region's capability to benefit from the opportunities provide by the Internet. Factors considered in the EIU rankings include the following: connectivity and technology infrastructure, business environment, consumer and business adoption, legal and policy environment, social and cultural infrastructure, and supporting e-services.

In January 2004, questionnaires were distributed to one hundred and fifty undergraduate students who major in accounting in Hong Kong SAR. One hundred and forty questionnaires were returned but one was unusable because of missing data. A similar survey was conducted in Australia in September 2004. Questionnaires were distributed to sixty-two postgraduate students. Forty-two were returned. Participation in the study was voluntary and no incentive was provided.

IV. Computer and Internet Usage

By March 2004, Australia has a population of 20 million [6]. Sixty-six percent of households in Australia have computers at home and among these five million households, 80% also have Internet access [5]. While 83% of Australian businesses use computers, only 23 percent of businesses have Web presence [4].

Similar situation of computer and Internet access in households was found in Hong Kong SAR. By 2004, Hong Kong SAR has a population of 6.8 million [13]. Sixty-eight percent of households in Hong Kong SAR have computers at home and nearly all these household (89%) have Internet access [14]. Nevertheless, the penetration rate of computer and Internet in the business sector is much lower in Hong Kong SAR than Australian businesses. Only 55% of Hong Kong SAR businesses use computers. The percentage of Web presence is even lower with only 14% [15].

The Hong Kong SAR government introduced a new multi-application smart identity card to its residents in August 2003. In addition to immigration purposes such as facilitating automated immigration clearance at border control points, a Hong Kong SAR smart identity card includes several non-immigration applications. Residents can now use the digital certificates embedded in their identity cards to update or check personal data kept by the government. With the embedded digital certificates, residents can encrypt email messages, conduct on-line share trading and on-line betting etc. [23]. Residents can use the digital certificate free for one year because the Hong Kong SAR government wants to encourage its people to adopt electronic commerce [32]. By the beginning of August 2004, over 420,000 smart identity card holders have opted for the free digital certificate [22]. This figure equals to around six percent of the population.

A high Internet connectivity rate or even ownership rate of digital certificate does not necessarily lead to individuals' acceptance of electronic commerce. The Finnish government issued a voluntary electronic identification card (EID) to its residents in 1999 [11]. It offered a low-priced digital certificate at 10 Euros to its residents. Nevertheless only ten percent of Finns were willing to pay for the digital certificate. It is unclear how many Finns use the certificates in the end [9]. Given the Finland example, this explorative study aims to investigate how the consumers in Pacific Asia perceive Internet security, how much they know about Internet security, and how ready they are in using digital certificates for electronic commerce transactions.

V. Results

V.1 Demographics

A total of 181 cases were used in the analysis. About two-third of respondents were female and the average age of respondents was 21.7. Furthermore, about two-third of respondents had five to eight years experience of using computer. The mean of Internet experience was 5.46 years. Nearly all respondents had computers at home (96.1%). A breakdown of the demographics of the two samples is shown in Table 1.

Among the 139 Hong Kong SAR respondents, 72% were female and 28% were male. They aged from 20 to 23. The average age was 20.8. Two-third of respondents had five to

eight years' experience of using computer. On average, respondents had 5.3 years experience of using the Internet. Ninety-nine percent had computers at home. Forty-five percent of Australia's 42 respondents were female and 55% were male. The Australian respondents had a wider age range from 21 to 37. About one-third of the respondents aged between 21 and 23. Their average age was 24.79. Similar to the Hong Kong SAR respondents, nearly two-third of the Australian respondents had five to eight years' experience of using computer. The ownership rate of home computer in Australia was slightly lower with only 86%. Yet they appeared to have more experience of using the Internet with an average of 6 years.

Table 1 Demographics of Hong Kong SAR and Australian respondents

Demographic profile	Hong Kong SAR	Australia	Mann-Whitney U-Test	
			Z-value	Sig (2-tailed)
Sample size	139	42		
Gender				
…Female	100 (71.9%)	19 (45.2%)		
…Male	38 (28.1%)	23 (54.8%)		
…Missing	1 (0.7%)	0 (0%)		
Age			-9.461	0.000***
…Mean	20.8	24.79		
…Min	20	21		
…Max	23	37		
Computer experience			-1.963	0.05*
…Mean	3.73	4.10		
… 1-2 years	2 (1.4%)	0 (0.0%)		
…3-4 years	17 (12.2%)	2 (4.7%)		
…5-6 years	51 (36.4%)	12 (28.6%)		
…7-8 years	41 (29.3%)	16 (38.1%)		
…9-10 years	13 (9.3%)	7 (16.7%)		
… 11-12 years	5 (3.6%)	2 (4.7%)		
…>12 years	10 (7.1%)	3 (7.2%)		
…Missing	1 (0.7%)	0 (0%)		
Home computer				
… Yes	138 (98.6%)	36 (85.7%)		
…No	1 (0.7%)	6 (14.3%)		
…Missing	1 (0.7%)	0 (0%)		
Internet experience (years)			-2.993	0.003**
…Mean	5.3	6.07		
…Min	2.0	2.0		
…Max	10.0	12.0		

*** significant at 0.001 level; ** significant at 0.01 level; * significant at 0.05 level

Statistical tests were conducted to compare the demographic features of the two samples. As data do not fulfill the assumptions of t-test, Mann-Whitney U test was used. The results of U-test show that Australian respondents were relatively older and had more computer and Internet experience than Hong Kong SAR respondents.

V. 2 Perceptions and knowledge

In addition to providing demographic details, respondents were asked to indicate the following in the surveys in a seven-point Likert scale: 1 indicates none, very insecure or very unlikely; 7 indicates very well, very secure or very likely.

- perception of Internet security
- self-assessed level of knowledge of Internet security
- self-assessed level of knowledge of public key infrastructure (PKI)
- self-assessed level of knowledge of certification authorities (CA)
- self-assessed level of knowledge of digital certificates
- intention to use digital certificate to encrypt emails
- intention to use digital certificate to access Internet banking services
- intention to pay fees to acquire/keep digital certificate

In view of the demographic differences noted above, responses of two samples on Internet security perception and knowledge were reported separately and Mann-Whitney U-test was used to investigate the difference across the two regions. Table 2 shows the comparison results. Overall, there was no significant difference between the two samples in terms of their perceptions and knowledge of the Internet security, and their intentions to use digital certificates. Respondents in both regions have a similar perception of the Internet security and perceived the Internet to be neither very secure nor very insecure (mean=3.83 and 3.55). The average self-assessed knowledge of Internet security in general of the Hong Kong SAR respondents was 3.68 and only one respondent indicated he/she had no knowledge of Internet security. The average self-assessed knowledge of Internet security in general of the Australian respondents was 3.57. The differences between the two regions on Internet perception and knowledge were statistically insignificant.

Table 2 Perceptions and knowledge on Internet security

Items	Hong Kong SAR (mean)	Australia (mean)	Mann-Whitney U-Test	
			Z-value	Sig (2-tailed)
Perception of Internet security	3.83	3.55	-1.334	0.182
Knowledge of Internet security	3.68	3.57	-0.329	0.742
Knowledge of public key infrastructure (PKI)	2.35	2.86	-1.477	0.140
Knowledge of certification authorities (CA)	2.78	2.86	-0.270	0.978
Knowledge of digital certificate	3.29	2.90	-1.712	0.087
Intention to encrypt emails	3.15	2.71	-1.321	0.186
Intention to use digital certificates to access Internet banking services	3.57	3.83	-0.495	0.621
Intention to pay fees to acquire/keep digital certificates	2.46	2.54	-0.013	0.990

As the two samples showed no significant differences regarding their perceptions and knowledge, further analysis was conducted by aggregating all the respondents (Table 3). Interestingly, respondents' self-assessed knowledge of PKI (mean=2.46) in both regions was much lower than their self-assessed knowledge of Internet security (mean=3.66). Fifty-four Hong Kong SAR respondents indicated that they knew nothing about PKI. Such a discrepancy in knowledge existed also for respondents' self-assessed knowledge of certific-tion authorities and digital certificates. The respondents' average knowledge of certification authorities and digital certificates

were 2.80 and 3.21 respectively. With reference to Table 2, Hong Kong SAR respondents' average knowledge of digital certificates was slightly higher than the Australian counterparts (Hong Kong SAR= 3.29; Australia = 2.90). It is unsurprising that the Hong Kong SAR respondents had a higher average knowledge of digital certificate than the Australian counterpart because more people owned digital certificate in the samples. Nevertheless, such a difference is statistically insignificant.

Most respondents in both regions were not keen to use digital certificates. Although studies have described emails as a killer application for the Internet [20] and most respondents used electronic mails regularly, more than half of the respondents indicated that it was highly unlikely for them to use digital certificates to encrypt email (mean=3.04). Their intention to use digital certificates for Internet banking were slightly higher (mean=3.67). With a mean of 2.48, respondents were unlikely to pay fees to acquire digital certificates.

Table 3. Perceptions and knowledge on Internet security of all respondents

Items	Mean
Perception of Internet security	3.77
Knowledge of Internet security	3.66
Knowledge of public key infrastructure (PKI)	2.46
Knowledge of certification authorities (CA)	2.80
Knowledge of digital certificate	3.21
Intention to encrypt emails	3.04
Intention to use digital certificates to access Internet banking services	3.67
Intention to pay fees to acquire/keep digital certificates	2.48

The Friedman test was then used to further examine the different types of self-assessed Internet security knowledge (Table 4). The results show that the levels of self-assessed Internet security knowledge were inconsistent (Chi-square=129.67). Further analysis shows that both Hong Kong SAR and Australian respondents' self-assessed levels of knowledge of Internet security in general were significantly higher than the others.

Table 4. Within-group comparison of Internet security knowledge

Items	Mean Rank
Knowledge of Internet security	3.14
Knowledge of public key infrastructure (PKI)	1.91
Knowledge of certification authorities (CA)	2.28
Knowledge of digital certificate	2.67
Friedman Test	
Chi-Square	129.67
Significance	0.000***
*** significant at 0.001 level	

Likewise, the Friedman test was used to examine respondents' intentions to use and acquire digital certificates (Table 5). The results show that respondents' intentions were inconsistent. Respondents were more likely to use digital certificates for Internet banking instead of email application. More importantly, their intentions of using digital certificates were higher than their intention to acquire the certificates.

Table 5. Within-group comparison of intentions

Items	Mean Rank
Intention to encrypt emails	2.02
Intention to use digital certificates to access Internet banking services	2.30
Intention to pay fees to acquire/keep digital certificates	1.68
Friedman Test	
Chi-Square	29.135
Significance	0.000***
*** significant at 0.001 level	

As this is an explorative study, we also examined the correlation among respondents' different perception and knowledge measurement items. Results of Spearman's Rho indicate that respondents' perception of Internet security was not related to their levels of knowledge and was only slightly correlated with their intention of using digital certificates for Internet banking. Nonetheless, their intentions to use digital certificate was significantly correlated to their levels of knowledge in Internet security.

VI. Discussions and Conclusions

In summary, the results of the study show that respondents were unsure how secure Internet is. Moreover, their self-assessed knowledge on Internet security was relatively low. In a Likert scale of 7, their lowest means of self-assessed knowledge was only 2.46. Similarly their intentions to use digital certificates were low with means between 3.04 and 3.67. Comparisons of two groups show that other than demographic differences, there was no significant difference between the two samples in any measurement item. That is, respondents in both regions have similar level of e-literacy and readiness to use digital certificates.

Further data analyses indicate that the self-assessed knowledge of several key concepts relating to Internet security (PKI, CA and digital certificates) of respondents in both Australia and Hong Kong SAR was significantly lower than their self-assessed knowledge of Internet security as a whole. Such inconsistency raises an interesting question: did consumers in Australia and Hong Kong SAR really know about Internet security or did they over-estimate their understanding? While one may argue that such overconfidence phenomenon is unsurprising, so far no empirical data was provided by any existing research to prove it.

Similar inconsistency was found over their intentions to use and acquire digital certificates. While the means of intention to use digital certificates were between 3.04 and 3.67, their intention to pay fees to acquire or keep digital certificate was significantly lower (mean=2.48). Results indicate that respondents might have intentions to use digital certificates, but they were not interested in paying fees to acquire the certificates. Although the residents in Hong Kong SAR will be given free certificates, they were as unlikely as their Australian counterparts to use the certificates. Results also suggest that between the two types of digital certificate application, respondents were more

likely to use digital certificates for Internet banking and did not concern much about confidentiality of their emails.

The results of the study are useful to Internet vendors as they reflect the level of e-literacy and consumers' intentions to use digital certificates in Internet transactions in Pacific Asia. Consumers need not be experts in Internet security but a basic understanding is necessary [16]. As respondents in both regions were university students, one may argue that generalization of conclusions should not be extended beyond this particular group of consumers. Nonetheless, being the "elites" of societies, if university students do not understand the concept of Internet security, how likely is it for the other consumers to understand it? As results indicate that respondents had low intention to pay for digital certificates, we recommend that if governments want to encourage e-commerce, they should provide free digital certificates to their residents. Moreover, results show that consumer's knowledge of Internet security is significantly related to their intentions to conduct Internet transactions. We recommend that in addition to promoting more digital certificate applications, governments should provide more education on Internet security to residents. People other than security professionals or students who major in computer science or information systems should have opportunities to learn about this topic. By understanding what digital certificates are, how they work and their pros and cons, consumers may be more willing to engage themselves in electronic commerce. With regard to further research in this area, researchers may consider developing a conceptual model and examine the interrelations among consumers' perception, knowledge and intention.

References

[1] ActiveMedia Research LLC. *Seventh Annual Survey of Online Commerce*, Peterborough, NH: ActiveMedia Research LLC, 2000.

[2] Ahuja, M., Gupta, B. & Raman, P. "An Empirical Investigation of Online Consumer Purchasing Behavior," *Communications of the ACM*, 2003, 46(12), 145-151.

[3] Arnfield, R. "Banking on Digital Certificates to Prevent UK Payment Fraud," *Infosecurity Today*, 2004, 1(3), 16-18.

[4] Australian Bureau of Statistics (ABS). *Business Use of Information Technology 8129.0*, 2002-2003a.

[5] Australian Bureau of Statistics (ABS). *Household Use of Information Technology 8146.0*, 2002-2003b.

[6] Australian Bureau of Statistics (ABS). *Australian Demographic Statistics 3101.0*, 2004.

[7] Aytes, K. & Connolly, T. "A Research Model for Investigating Human Behavior Related to Computer Security," *Ninth Americas Conference on Information Systems*, 2003, 2027-2031.

[8] Backhouse, J. "Assessing Certification Authorities: Guarding the Guardians of Secure E-commerce," *Journal of Financial Crime*, 2002, 9(3), 217-226.

[9] Balaban, D. "Digital Signature Cards: For Professionals Only?" *Card Technology*, 2003, 8(3), 28-30, 32, 34.

[10] Barnes, B. H. "Computer Security Research: A British Perspective," *IEEE Software*, 1998, 15(5), 30-32.

[11] Bowen, C. "Government 101: Smart Card IDs. Lessons Learned," *Card Technology*, 2002, 7(13), 34-36, 40-44.

[12] Bruschi, D., Curti, A. & Rosti, E. "A Quantitative Study of Public Key Infrastructures," *Computers & Security*, 2003, 22(1), 56-67.

[13] The Census and Statistics Department (CSD). "Hong Kong Population Projections 2004-2033," *Hong Kong Monthly Digest of Statistics*, Hong Kong SAR Government, 2004a.

[14] The Census and Statistics Department (CSD). *Household Survey on Information Technology Usage and Penetration*, Hong Kong SAR Government, 2004b.

[15] Census and Statistics Department (CSD). *Penetration and Usage of Information Technology in the Business Sector*, Hong Kong SAR Government, 2004c, http://www.info.gov.hk/censtatd/eng/hkstat/fas/st/penetration.htm.

[16] Charrot, T. "What's Wrong with Public Key Cryptography?" *Computer Fraud & Security*, 2001, 2001(7), 12-15.

[17] Chen, K., Lee, H. & Mayer, B.W. "The Impact of Security Control on Business-to-Consumer Electronic Commerce," *Human Systems Management*, 2001, 20(2), 139-147.

[18] Economist Intelligence Unit (EIU). *The 2003 E-readiness Rankings*, 2003.

[19] Forno, R. & Feinbloom, W. "PKI: A Question of Trust and Value," *Communications of the ACM*, 2001, 44(6), 120.

[20] Goldsborough, R. "E-mail: The Net's Killer Application," *Computer Dealer News*, 1999, 15(48), 21.

[21] Greenstein, M. & Vasarhelyi, M.:*Electronic Commerce: Security, Risk Management, and Control*, McGraw-Hill, Irwin, second edition, 2002.

[22] Hongkong Post: Press Release, 2004a, http://www.hongkongpost.gov.hk/news/press/39.html.

[23] Hongkong Post *Using E-cert on Smart ID Card*, , 2004b, http://www.hongkongpost.gov.hk/activity/smartid/carduse/index.html.

[24] Hunt, R. "Technological Infrastructure for PKI and Digital Certification," *Computer Communications*, 2001, 24(14), 1460-1471.

[25] Janbandhu, P.K.& Siyal, M.Y. "Novel Biometric Digital Signatures for Internet-based Applications," *Information Management & Computer Security*, 2001, 9(5), 205-212.

[26] Jaweed, S. "Could There Ever be a Unitary Digital Certificate?" *Information Security Technical Report*, 2003, 8(3), 36-44.

[27] Kim, D.J., Ferrin, D.L & Raghav, R.H. "Antecedents of Consumer Trust in B-to-C Electronic Commerce," *Ninth Americas Conference on Information Systems*, 2003, 157-167.

[28] Korzaan, M.L., Rutner, P.S. "Intentions to Purchase and the Online Experience," *Ninth Americas Conference on Information Systems*, 2003, 314-323.

[29] Landrock, P. "Security - The Building Block for E-commerce Growth," *Computer Fraud & Security*, 2002, 2002(9), 7-8.

[30] Lee, Y. & Qiang, Q.P. "Chinese Perceptions on Website Design Quality," *Ninth Americas Conference on Information Systems*, 2003, 1134-1138.

[31] Lim, N. "Consumers' Perceived Risk: Sources versus Consequences," *Electronic Commerce Research and Applications*, 2003, 2(3), 216-228.

[32] Mak, S. "Enhancing Information Security with Digital Certificate and Public Key Infrastructure," *Presentation at Managers Forum-IT Series*, 2003.

[33] Mott, S. "The Second Generation of Digital Commerce Solutions," *Computer Networks*, 2000, 32(6), 669-683.

[34] Moulton, R.T. & Moulton, M.E. "Electronic Communications Risk Management: A Checklist for Business Managers," *Computers & Security*, 1996, 15(5), 377-386.

[35] Odekerken-Schröder, G. & Wetzels, M. "Trade-offs in Online Purchase Decisions: Two Empirical Studies in Europe," *European Management Journal*,2003, 21(6), 731-739.

[36] Tan, H.S.K. "E-fraud: Current Trends and International Developments," *Journal of Financial Crime*, 2002, 9(4), 347-354.

[37] Ungureanu, V. "Formal Support for Certificate Management Policies," *Computers & Security*, 2004, 23(4), 300-311.

[38] Vijayasarathy, L.R. "Predicting Consumer Intentions to Use On-line Shopping: The Case for an Augmented Technology Acceptance Model," *Information & Management*, 2003, 41(6), 747-762.

[39] Ward, M. "Digital Certificates and Payment Systems," *Information Security Technical Report*,1998, 2(4), 23-31.

[40] Yang, Z. & Jun, M. "Consumer Perception of E-service Quality: From Internet Purchaser and Non-purchaser Perspectives," *Journal of Business Strategies*, 2002, 19(1), 19-41.