ICEB 2004 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-5-2004

Internet Security and Digital Certificates: How Much Do You Know About Them?

Nena Lim

Internet Security and Digital Certificates:
How Much Do You Know About Them?

Nena Lim

UQ Business School, The University of Queensland, Brisbane, QLD 4072, Australia
n.lim@business.uq.edu.au

ABSTRACT

The objective of this paper is to investigate to what extent the general public knows about Internet security and digital certificates as well as how likely they would use digital certificates if the certificates are free and ready for them to use. The Hong Kong SAR government introduced a new multi-application smart identity card to its residents in August 2003. As the government wants to encourage its residents to adopt electronic commerce, residents can choose to embed a free digital certificate in their smart identity cards. A survey was conducted in Hong Kong SAR in January 2004 and one hundred and forty questionnaires were returned. Results show that the respondents' self-reported knowledge of several key concepts related to Internet security were inconsistent. Moreover, respondents did not seem to have much understanding of the usefulness of the digital certificates nor did they appear to be too keen to use the digital certificates for electronic transactions.

Keywords: digital certificate, electronic certificate, PKI, Hong Kong SAR smart identity card

1. INTRODUCTION

Internet security has been repeatedly shown to be a major worry of consumers and an obstacle for the success of electronic commerce [1-3]. One of the solutions researchers and businesses have found for this problem is the adoption of digital certificates (also known as electronic certificates) for Internet communications and transactions. A digital certificate establishes an individual or an organization's identity in the cyber world. Issued by a certification authority (CA), 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 mechanism of digital certificates relies on the public key infrastructure (PKI) to achieve on-line authentication. Under the PKI, individuals with no prior relationship can achieve confidentiality and authentication when they swap information over the Internet or conduct electronic commerce transactions [1].

Although PKI has already existed for several decades, many consumers still hesitate to get involved in electronic commerce transactions. Why? One possible explanation is that although public key encryption algorithms have progressed quickly since 1970s [4], consumers do not feel any safer because they do not know how PKI works nor do they understand the protection digital certificates can offer. The objective of this paper is to investigate to what extent the general public knows about Internet security and digital certificates as well as how likely they would use digital certificates if the certificates are free and ready for them to use.

2. HONG KONG SAR SMART IDENTITY CARD

The Hong Kong Special Administration Region (SAR) has a population of 6.8 million in mid-2003 [5]. Sixty-eight percent of households in Hong Kong SAR have personal computers and nearly all these households (89%) have Internet access [6]. 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 also 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 also encrypt email messages, conduct on-line share trading and on-line betting etc. [7]. Residents can use the digital certificate free for one year because the Hong Kong SAR government wants to encourage people to adopt electronic commerce [8]. Despite the good intentions of the government, do the Hong Kong SAR residents understand what digital certificates are? Are they ready to trust and hence utilize the digital certificates for electronic commerce transactions? To what extent will the goal of Hong Kong SAR government of creating a critical mass for electronic commerce be achieved?

By the beginning of August 2004, over 420,000 smart identity card holders have opted for the free digital certificate [9]. This figure equals to only six percent of the entire population. Assuming more people opt for the digital certificate after the promotion of some renowned celebrities, the key issue one should remember is: a high Internet connectivity rate or even ownership rate of digital certificate does not necessarily lead to individuals' acceptance of electronic commerce.

Citizens in Finland do not consider it worthwhile to pay 10 Euros for a digital certificate [10]. Similarly, a low acceptance rate of digital certificate was reported in Germany. Less than one percent of students in a German university applied for a smart card which has a digital certificate embedded in it. The cards and card readers were heavily subsidized by the university. Yet even computer science students did not show too much interested in the cards. Those who got the cards only used them infrequently [10].

3. METHODOLOGY

To investigate their understanding of Internet security and digital certificates as well as their readiness in using the free digital certificates, a survey of Hong Kong residents was conducted in January 2004. One hundred and fifty questionnaires were distributed to associate degree students who have enrolled in an advanced accounting course at the City University of Hong Kong. One hundred and forty questionnaires were returned. Among the respondents, 72 percent were female and 27 percent were male. They aged from 20 to 23. The average age was 20.8. Most respondents had five to eight years experience of using computer and five to six years experience of using the Internet. Ninety-nine percent had computers at home.

4. RESULTS

In a seven-point Likert scale, the average self-reported knowledge of Internet security in general was 3.7 and only one respondent indicated he/she had no knowledge of Internet security. Yet interestingly respondents' self-reported knowledge of PKI was much lower with an average score of only 2.3. Fifty-four respondents indicated that they knew nothing about PKI. Similar results exist for respondents' self-reported knowledge of certification authorities and digital certificates. The respondents' average knowledge of certification authorities and digital certificates were 2.35 and 3.3 respectively. The relatively higher self-rating of digital certificate is unsurprising because ten percent of the respondents already owned valid digital certificates. These people must had obtained the certificates on their own because according to the government schedule it was not their turns to apply for the new identity cards yet. The results raise an interesting question on the inconsistency of respondents' self-reported knowledge. Did people really know about Internet security or did they over-estimate their understanding?

There is no significant difference between the "have" and "have not" groups of digital certificates in all aspects except their knowledge of digital certificates. Out of the 125 respondents who did not have a valid digital certificate, two-thirds did not know what applications digital certificates could provide. After being told the applications they could use, these respondents were not keen to use those applications. For example, while 119 respondents use electronic mails regularly, only 20 percent indicated that they might use the digital certificates to encrypt their emails. Furthermore, two-thirds of these respondents were not aware that they would need to have a smart-card reader to use the free digital certificate embedded in their smart identity card for on-line applications. Once they were aware of the equipment requirement, 95 percent indicated they were either unsure or unlikely to purchase a smart card reader. Such results are unsurprising as smart card readers have been shown to be a major obstacle of smart card adoption [10]. Although 40 percent of respondents indicated they would opt to include the free digital certificates into their identity cards, 93 percent of them would not pay the annual fee themselves once the certificates expire after one year. Results also indicate that those who were willing to buy smart card readers are more likely to pay annual fees (r = 0.425).

5. CONCLUSIONS

In summary, results of this study show that the self-reported knowledge of respondents of several key concepts related to Internet security were inconsistent. It is doubtful how much they really know. Moreover, respondents did not seem to have much understanding of the usefulness of the digital certificates embedded in their new smart identity cards and they did not appear to be too keen to use the digital certificates for electronic transactions. To achieve its objective of promoting electronic commerce transactions, we recommend the Hong Kong SAR government to consider further educating its residents on Internet security because results of this study suggest that the general public in Hong Kong is unlikely to make good use of the digital certificates. While some forms of public education such as exhibitions were conducted in the past, results suggested that more should be done. For example, promotions of useful applications such as on-line submission of tax returns can be used to attract usage of digital certificates. Moreover, more advertising and education are required to familiarize residents with the benefits of digital certificates. One way to educate the general public is to start from students, from primary schools to tertiary institutions, so that the next generation will be more ready to face the electronic age.

REFERENCES

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

[2] Lim, N., "Consumers' perceived risk: Sources versus Consequences", *Electronic Commerce Research and Applications"*, Vol. 2, No. 3, pp216-228, 2003.

[3] Vijayasarathy, L. R., "Predicting consumer intentions to use on-line shopping: The case for an augmented technology acceptance model", Information & Management, Vol. 41, pp747-762, 2004.

[4] Schneider, G. P., *Electronic Commerce*, Course Technology, Thompson, 2003.

[5] The Census and Statistics Department, "Hong Kong populatin projections 2004-2033", *Hong Kong Monthly Digest of Statistics*, Hong Kong SAR, 2004.

[6] The Census and Statistics Department, *Household survey on information technology usage and penetration*, Hong Kong SAR, 2004.

[7] Hongkong Post, "Using e-cert on smart ID card" http://www.hongkongpost.gov.hk/activity/smartid/carduse/index.html.

[8] Mak, S. "Enhancing information security with digital certificate and public key infrstructure", *Presentation at Managers Forum-IT Series*, 2003.

[9] Hongkong Post, *Press Release*, http://www.hongkongpost.gov.hk/news/press/39.html, Hong Kong Post, 2004.

[10] Balaban, D. "Digital signature cards: For professionals only?", *Card Technology*, Vol. 8, No. 3, pp28-30, 32, 34, 2003.