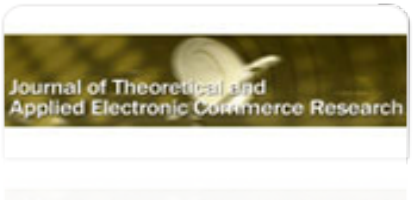

Journal of Theoretical and Applied Electronic Commerce Research
E-ISSN: 0718-1876
ncerpa@utalca.cl
Universidad de Talca
Chile

Singh, Supriya
The Social Dimensions of the Security of Internet banking
Journal of Theoretical and Applied Electronic Commerce Research, vol. 1, núm. 2, august, 2006, pp. 72-78
Universidad de Talca
Curicó, Chile

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

The Social Dimensions of the Security of Internet banking

Supriya Singh

RMIT University/Smart Internet Technology Cooperative Research Centre, RMIT Business,
supriya.singh@rmit.edu.au

Received 02 December 2005; received in revised form 24 April 2006; accepted 26 June 2006

Abstract

This paper examines the users' perspective on the security of Internet banking in Australia within the social context. This user-centered design approach supplements the technological and industrial approaches to security. The user-centered research on banking was conducted at the Royal Melbourne University of Technology University and Griffith University, both of which are part of the Smart Internet Technology Cooperative Research Centre. We conclude that the most effective way to increase the perception of Internet banking security is to increase ease of use, convenience, personalisation and trust. Without the perception of security, there will be little trust in banking and transactions on the Internet. This will impede the use of Internet banking and e-commerce which are increasingly important aspects of the nation's critical infrastructure.

Key words: Internet banking, security, users' perspective, trust, privacy

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

1 Introduction

Banks want customers to feel Internet banking is secure, so that Internet transactions can substitute for a greater part of the more costly branch, telephone, ATM and EFTPOS transactions. Internet banking is now an integral part of banks' business model. Banks also want to retain the mantle of a trusted organization. In the United States, banking sites are trusted by 68 per cent of all Internet users and more so by those who use Internet banking [25]. Not achieving a perception of security will have the wider effect of reducing customers' trust in banks, electronic banking and more particularly Internet transactions. It is however impossible to ensure perfect security, particularly as the unsupported PC was not designed for secure Internet commercial transactions [2]. PC manufacturers and suppliers of related products have clearly stated that the PC is not suitable for home banking. This is even more true as criminal attacks on Internet banking have become more sophisticated, particularly with the development of key logger software [2], [21].

Banks addressed the problem of imperfect security in the case of credit cards by capping customers' liability in case of fraudulent use. For e-commerce transactions that involve purchase and sale, banks in Australia have laid the responsibility of fraudulent use on the merchants. Bank contracts with customers however, are ambivalent about the responsibility for the security of Internet banking transactions. Banks are active in moving customers to Internet banking through lower fees and bank branch closures, while at the same time also warning customers of the need to be careful. Though Australian Standards relating to Electronic Funds Transfer and the EFT Code of Conduct provide consumer protections, the protections for Internet banking have still to be tested in court. McCullagh and Caelli document a case where the National Australia Bank reimbursed one of its customers whose Internet banking from a cyber café was intercepted by a Trojan key logger [21].

2 Testing the responsibility for security: The AHLO case

The first case testing the responsibility for the security of Internet banking is pending in the Florida State Court. (There has been no further news since May 2005 of it on the Internet in terms of commentary). This case is important for it will establish for the first time whether the responsibility for security of Internet banking lies with the customer or the bank. In April 2004, AHLO Inc a small printer and ink business in Miami, lost US$ 90,348.65, in a Bank of America account through a fraudulent transfer from the company's account to an account with the Parex Bank in Riga, Latvia. AHLO alleges it advised BOA, but the bank did not take action for some 19 hours. By this time $US 20,000 had been withdrawn from Parex Bank. BOA argues that it does not have the legal authority to have the remainder transferred to AHLO. AHLO is proceeding against the bank alleging in part that there has been a breach of fiduciary duty and that the bank has not acted in good faith. BOA is arguing that the problem lay with the security of AHLO's PC rather than its own networks and so the responsibility rests with AHLO. The Secret Service found that AHLO's computer was infected with the Trojan called Coreflood, though it does not state it was the cause [18], [21].

There are divided opinions as to the bank's responsibility. The bank may win the case, but weakening consumer confidence makes the bank's legal strategy questionable. Making small businesses responsible for the technical security of the PC may not be a viable option. On the other hand paying out AHLO may open the floodgates [31]. Ramasastry, a former staff attorney for the New York Federal Reserve Bank, wrote that "the legal duty of banks to protect against hacking should be limited to their own networks - about which they are knowledgeable, and over which they have control" [8]. The AHLO case may be won or lost on issues of technical security of the business PC or the bank's responsibility for fraudulent Internet banking. But in the meantime Lopez, the owner of AHLO "has stopped using wire transfers" [18].

This is the background of the inherent conflict between the near impossibility of customers ensuring the ongoing and continuous security of the PC against advanced malware, and banks' policies relating to security. The story gets more complicated as one goes beyond technology and the law to take into account users' perspectives on Internet banking security. Section three surveys the developing literature on user-centred security. Section four draws upon a qualitative user-centered study of banking. In section five, there are concluding remarks about customers' perception of security being increased by addressing issues of trust, usefulness and personalization.

3 User-centered perspectives on security

The user-centred approach to security is still in its early stages. This approach places the user at the centre of security development. There has been welcome emphasis on aligning security and usability. But when the user is modeled on the developer of security systems, it is the expert user that is considered [6].

There has also been a focus on the psychological dimensions of security. Consequently issues of ease of use and cognitive load have become part of the discussion of security mechanisms. However, for the most part, the literature on user-centered security sees the user as an individual in an organizational context [26]. The literature to date has not adequately taken the social and cultural context into account. There has been some welcome work on the group context in organizations [12], [23] and 'social translucence' [1], [11]. But the field needs to expand in two directions.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

First, the domestic context of individual and shared activities in the household has become important as the Internet becomes a channel for daily activities. Second, these activities and values need to be studied in the field, rather than a lab, so that the social and cultural meaning of activities becomes apparent. As Tognazzini [33] says, "Both students and professors need to do field studies of real people working in real environments" (p. 46). It is only when people are studied in their social contexts rather than unattached individuals that some of the relevant social practices can be identified. The cultural meanings of activities also have to be taken into account. This is particularly true for online financial transactions as money is managed and owned in different ways in various cultures.

There are three strands to the debate. The first is that it is the usefulness of technology for a designated activity rather than technology itself that is at the centre of security. The second is to move from a focus on security to an emphasis on trust. Control and comfort with the transaction, together with a perception that the customer is being looked after, is essential for trust. The third is the close connection between privacy and the control of personal information. This emphasis on control of personal information connects security, trust, privacy and identity.

3.1 Usefulness and security

The connection between usefulness and technology is at the center of much of the developing user-centred perspectives on security. This connection focuses on three aspects: the primacy of the activity over technical aspects of security, usability of security solutions, and users' feelings of control.

Karat et al [16, p. 2] point out the primacy of the activity, saying "... the use of security and privacy solutions is generally not the user's main goal. Users value and want security and privacy functionality as secondary to completing their primary tasks".

Cranor and Garfinkel in their preface to *Security and Usability: Designing Secure Systems that People Can Use* [9] say,

> Many people believe that there is an inherent tradeoff between security and usability… if people are unable to use secure computers, they will use computers that are not secure. At the end of the day, computers that are theoretically secure but not usable do little to improve the security of their users… the converse is also true: systems that are usable but not secure are, in the end, not very usable either (pp. ix- x).

A focus on the psychological dimensions of security has emphasized ease of use [6]. The literature on passwords thus emphasizes cognitive load, that is the need to keep the password easy to use but difficult to guess. Bishop says "A password is a sequence of characters that confirms the user's identity" (pp. 2-3). Sharing of passwords is only considered in the context of insuring against a memory lapse.

There is also a narrower focus on the usability of security solutions. Schneier opens his book *Secrets and lies: Digital security in a networked world* with a *mea culpa* relating to his earlier book *Applied Cryptography* [27]. He says he was wrong to think that mathematics alone could ensure digital security. He did not take into account users and their context [28].

He says security is a multi-layered process, rather than a product. Reflecting on his earlier influential work, Schneier says,

> I came to security from cryptography, and thought of the problem in a military-like fashion. Most writings about security come from this perspective, and it can be summed up pretty easily: Security threats are to be avoided using preventive countermeasures" (p. 397).

He realised in 1999 that "…the fundamental problems in security are no longer about technology; they're about how to use the technology" (p. 398).

D'Hertefelt [10] also argues "that the feeling of security experienced by a user of an interactive system does not depend on technical security measures alone. Other (psychological) factors can play a determining role" (no page number noted). This research suggests that "the feeling of security experienced by a user of an interactive system is determined by the user's feeling of control of the interactive system."

Based on qualitative research towards making the website of an European airline more usable, they came up with the unexpected finding that "people's perception of security when doing on-line transactions depends on the simplicity of the site and on the availability of user support." D'Hertefelt noted:

> This observation puzzled us. Discussions about security on internet seem preoccupied with technical issues such as 128-bit encryption, secure sessions, authentication, digital certificates, secure sockets layer, etc. And we observe that people feel secure because... "it's easy"?

One approach which bridges the gap between security and usability is "the concept of integrated user-centered security engineering" [13]. Their investigation of existing security tools, like PGP (www.pgp.com), Signtrust Mail (www.signtrust.de), and freedom (www.freedom.com), showed that systems do not fail because of malfunction, but because they were too complex or difficult for users. The need was for "usable security" combining the processes of usability and security engineering.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

3.2 Trust and security

Trust is a wider concept than security. Trust however is difficult to define because it is nebulous and all-pervading. People speak of trust most clearly when they speak of a lack of trust. This is especially so in situations where there is a greater risk and where information is less easily available[30]. Issues of trust and the use of electronic money are increasingly being discussed [4], [15], [17], [19], [20], [30], [32].

It is important to disentangle the concepts of security and trust, because even "usable security" is not always a sufficient condition for trust. Friedman and Grudin emphasise the importance of human values establishing and maintaining trust for the effectiveness of the information infrastructure [12] . They say:

> The common good of our information infrastructure depends on designs through which users can establish and maintain trust and accountability. Without preserving such human values, users will be reluctant to embrace this infrastructure as a means for conducting their daily affairs -- commerce, communication, health, work, and education (p. 213).

Where these values of trust are not at the centre of security systems in organizations, security mechanisms will be bypassed or subverted. Sharing information is essential for work in an organization and these preferences need to be taken into account [23]. Sasse and Flechais also [26] say:

> In most current cases, existing trust relationships in an organization facilitate the breaking of security policies and practices. In fact... adhering to existing security policies can undermine social relationships within a group of peers. The authors argue.. that the organizational culture and the actual security should be designed to support both trust relationships and adherence to policy (p. 26).

Separating trust and security means distinguishing between "…issues of 'hard trust,' which involve authenticity, encryption, and security in transactions, and issues of 'soft trust,' which involve human psychology, brand loyalty, and user-friendliness..." [7, p. 21]. Singh and Slegers [30] unpack issues of soft trust and electronic money. They conclude that the user has to feel he or she is in control of the information, that he or she has comfort in the use of the service or channel. The dimension of caring is particularly important as a glue for trust in all cases, but particularly where the user does not have the expertise or ability to control the situation.

3.3 Privacy as the control of personal information

Lawyers, technologists, sociologists and psychologists have defined the concept of privacy in different ways. Privacy and security are often seen as synonymous, particularly when privacy is interpreted legally and technically as keeping intruders out of a person's business. However user centered studies of privacy have emphasized that privacy rests in the control of the sharing of personal information and presenting our version of ourselves [3], [24], [29]. Privacy does not equate with anonymity. It also does not mean being left alone. As Tognazzini [33] says, "Privacy considerations should be separate and distinct from security.. You can build highly secure systems that enhance, rather than reduce privacy" (p. 41). Karat et al [16] say:

> The intersection of human-computer interaction (HCI), privacy and security is emerging as a critical area for research amid the backdrop of recent world events. .... it is becoming increasingly clear that really making our systems secure and enabling appropriate attention to privacy issues will require more than just a technology focus (p. 1)..

Issues of privacy in the banking context focus strongly on the risk of losing money via the fraudulent use of the credit card and/or information related to Internet banking. As banks hold detailed personal information about a person's financial status, there is an additional concern that a leaking of this information could affect a person's representation of self.

The next section discusses a qualitative study of Australian consumers' perceptions of security within the context of how they bank.

4 Qualitative study of privacy and security in Australian banking

The aim of the qualitative study was to understand how Australian consumers perceived issues of security, identity, trust and privacy in banking. The study adopted the users' perspective where the emphasis was on the banking activity. Preliminary results of the study are presented, drawing on open ended interviews with 38 people in Melbourne and Brisbane, between April 2005 and September 2005. The people were identified and accessed through personal and professional networks. Our sample had nine men and 29 women; an even distribution across ages; a range of annual household income levels; a dominance (30 of 38) of those with a BA or higher degree, particularly in IT.

The "grounded" approach was chosen to understand how people manage their financial information across life stages [14]. We used N6, a computer program used code, sort , analyse and check the rigour of qualitative analysis [22].

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

4.1 Preliminary Results: Usefulness, convenience and security

Usefulness and convenience were the main factors leading to the use of Internet banking for 19 of our 38 participants.

Of the 19 who did not use Internet banking, two did not find it useful enough, 13 had an annual household income of less than AUS$50,000, and four did not use Internet banking because of a lack of security.

Fifteen of the nineteen who used Internet banking valued convenience and habit over concerns about privacy and security. They directed attention away from their not being totally satisfied with the security and privacy of the Internet. Some tried not to think of the risks because they felt they could not control these risks. They also used risk minimization techniques such as using credit cards with low limits, using a computer and network they saw as secure, or assuring themselves that the site had the sign of a lock to symbolize security.

Ellen, 35-44, an academic in part time work who has a household income of over AUS$100,000 says she likes the convenience and the immediacy of the Internet. She buys groceries online and does all her banking on the Internet. She thinks that hackers are going to be able to steal their money one day, “but at this stage I don't see it as a security problem”. She tries to be careful by keeping her passwords secure, and making sure she is on a secure site. She perceives the university server as secure. In the end she tries to stop being anxious by admitting nothing is totally secure. And if anything happened she feels she has the confidence to follow up and get the money back.

Laura, 25-34, with her own business in health services, has always banked using the Internet. Replying to questions about trust, privacy and security, she says, “I don’t know that I think about it a lot, because I think I don’t understand it enough. So I don’t think about it.…It’s completely hiding your head in the sand”. Others like Gillian, 35-44, a PhD student in IT and a household income of more than AUS$100,000, try and protect themselves by using the latest spyware, or having a credit card with a very low limit. She trusts the bank’s system “is secure”.

4.2 Trusting the bank

There is a comfort in dealing with the bank in a way that offers convenience and a greater control of current information about one’s money. But when the untoward happens, and the bank deals with the customer in a way that he or she finds caring, then the trust is often further enhanced. Dealing adequately with the unexpected and negative consequences are important for trust in online transactions [5].

Three of our 38 participants have experienced the fraudulent use of the credit card. Two of the three continue to use Internet banking because their problems with the credit card were satisfactorily resolved. Anita, now a housewife, 55-64, with a household income between $55,000 and $74,000 says $300 was withdrawn from her husband’s credit card. When he rang the bank as he was the primary card holder, the money was returned. This experience left Anita cautious about checking statements and she does not use a credit card on the Internet – choosing instead to use BPay. However, she regularly uses the Internet to monitor her accounts, transfer money and pay bills. She uses the Internet but worries about the security and keeps a constant eye on her finances. Her only strategy to lessen the risk is that of constant monitoring. She says, “I just hope that… nothing will happen. I just put .. full trust on.. the banks that.. they are doing their best…”

Amber, 28, with a household income below $50,000 says her partner had money taken from his credit card. He rang the bank and they refunded the money. This experience of credit card fraud and its subsequent solution has enhanced the cardholder’s feeling of trust in the bank. Dora, 35-44, an academic also had a problem with the fraudulent use of her credit card when in South East Asia. She says this is one of the reasons she doesn’t use Internet banking.

4.3 Privacy, personalisation and responsiveness in the bank

For our participants, comfort in the privacy of personal information with the bank, was not based on the legal privacy policies. Only three of the 38 people in our sample read the privacy policy. For the most part the participants felt they could not hold the bank to account because of the privacy policy. Three others saw it was the bank who used the Privacy Policy as a way to restrict their access to information and personalise their accounts. This was particularly the case with joint accounts, where the bank imposed a hierarchical structure of the primary and secondary account or card holder. It was the primary account holder who had the right to change account information. The bank’s actions did not take into account the wishes of the couple themselves, for more equal control.

Gillian, 35-44, a PhD student in IT, with a household income between AUS$75,000-$99,999 said she and her husband found themselves in the awkward situation where the bank would not accept her changing the contact details for the credit card for both herself and her husband. She is the one who has the online log-on for the credit card. This is so that they can minimise the number of passwords they have. She says she emailed and asked the bank “…to change our address, our postal and home address because we had moved. They changed mine but they wouldn't change his, even though I'm a secondary card holder”.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

This meant her husband had to ring the bank to give Gillian permission to change the credit card details. She tried to find out if she could change the details in the future and the bank said "No. Every time you want to make any changes, he has to ring and authorize you to talk to me again". Gillian says,

> All we had to do was tell his name, his date of birth, his mother's maiden name and the account number….If you knew the person you could quite possibly know the mother's maiden name. …To me that is not as secure as being able to send an encrypted email through a banking system. There is no point fighting them. They don't listen.

5 Findings and conclusion

This paper has presented three strands from the nascent literature on user-centred security, trust and privacy, which are important for Internet banking and e-commerce. It then presented interim results from a qualitative study of privacy and security in Australian banking. We found that people focus on a designated activity such as banking or purchase, rather than the technologies used to enhance security. Trust in the organisation or the medium is at the center of people's feelings of control and comfort. Users' perception of control is also at the centre of issues of privacy. Convenience and ease of use are at the center of customers' positive experience of Internet banking. The usefulness of Internet banking together with trust that the bank will look after customers' interests, overcomes concerns about security and privacy. The concerns with Internet banking rest more on customers' perception of inadequate control over their personal information and personalisation of banking.

Providers of online services need to focus on giving the user control over the transaction and the activity. There need to be acceptable mechanisms in place to correct the situation if something untoward happens with the transaction. It is this assurance that enables people to use credit cards with comfort, despite known problems, and sometimes experience, with credit card fraud. The technologies that enable security are important, but most users cannot judge the effectiveness of these technologies. Moreover, some of the most expert users have good grounds to doubt that these technologies can guarantee security.

The literature and the qualitative study leads to the conclusion that providers of online services can increase customers' perception of security in three ways. The first is to increase the convenience and usefulness of online transactions. The second is to have customers believe the provider will not allow them to suffer fraudulent transactions. The third step is to give customers a more personalised experience of online transactions by giving them greater control of their transactions and information. All security solutions, irrespective of their technological base, need to provide customers with this ease of use, trust and personalization of online transactions.

A change in the mind-set of security designers is already beginning with the emphasis on user-centered security. The next step is to address the needs of people in their social and cultural aspects, particularly in their domestic environments. It is this emphasis on the social dimensions of security that will enable people to take the Internet for granted and use it as a tool for their everyday activities.

Acknowledgments

I would like to gratefully acknowledge the support of the Smart Internet Technology Cooperative Research Centre. In particular my thanks go to Jenine Beekhuyzen, Anuja Cabraal, Gabriele Hermansson, Margaret Jackson, Jan Browne, Lesa Beel and Doug Lorman who helped conduct the qualitative study. This study was part of a larger project on Trust, Security, Privacy and Identity in the Smart Internet Technology Cooperative Research Centre.

References

[1] M. S. Ackerman, The intellectual challenge of CSCW: The gap between social requirements and technical feasibility, in Human-Computer Interaction in the New Millennium, J. M. Carroll, Ed. New York: ACM Press, 2002, pp. 303-324.
[2] G. Adamson, The Mixed Experience Of Achieving Business Benefit From The Internet -A Multi-Disciplinary Study, in Business Information Technology. Melbourne: RMIT University, 2003.
[3] P. Agre, Introduction, in Technology and Privacy: The New Landscape, P. Agre and M. Rotenberg, Eds. Cambridge, Mass.: The MIT Press, 1998, pp. 1-28.
[4] T. Barr, A. Knowles, and S. Moore, Taking users up the value chain: Australian Internet research, Smart Internet Technology Cooperative Research Centre, Melbourne February 2004.
[5] G. Bewsell, Mangoes and Chilli Peppers: A Domain Study of Online Trust in eAuctions, presented at 16th Australasian Conference on Information Systems, Sydney, 2005.
[6] M. Bishop, Psychological acceptability revisited, in Security and Usability: Designing Secure Systems that People Can Use, L. F. Cranor and S. Garfinkel, Eds. Sebastopol, CA: O'Reilly, 2005, pp. 1-11.
[7] D. Bollier, The future of electronic commerce: A report of the Fourth Annual Aspen Institute Roundtable on Information Technology, The Aspen Institute, Aspen, Colorado 1996.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 72 – 78

This paper is Available online at
www.jtaer.com

[8] S. Cocheo, Privacy rumblings grow louder: prompted by recent publicity over data breaches, Congress, state houses, and, increasingly, the courts are considering cases and proposals that could impact banks., vol. 2006: ABA Banking Journal:, 2005.
[9] L. F. Cranor and S. Garfinkel, Preface, in Security and Usability: Designing Secure Systems that People Can Use, L. F. Cranor and S. Garfinkel, Eds. Sebastopol, CA: O'Reilly, 2005, pp. ix-xviii.
[10] S. D'Hertefelt, Trust and the perception of security, vol. 2004, 2000.
[11] T. Erickson and W. A. Kellogg, Social translucence: Designing systems that support social processes, in Human-Computer Interaction in the New Millennium, J. M. Carroll, Ed. New York: ACM Press, 2002, pp. 325-345.
[12] B. Friedman and J. Grudin, Trust and accountability: preserving human values in interactional experience, presented at CHI 98 conference summary on Human factors in computing systems, Los Angeles, California, United States, 1998.
[13] D. Gerd tom Markotten, User-Centered Security Engineering, vol. 2004, 2002.
[14] B. G. Glaser and A. L. Strauss, The discovery of grounded theory: Strategies for qualitative research. Chicago: Aldine, 1967.
[15] R.-L. Hsiao, Technology fears: distrust and cultural persistence in electronic marketplace adoption, The Journal of Strategic Information Systems, vol. 12, pp. 169-199, 2003.
[16] C.-M. Karat, J. Karat, and C. Brodie, Why HCI research in privacy and security is critical now, Human-Computer Studies, vol. 63, pp. 1-4, 2005.
[17] J. Lee and A. Allaway, Effects of personal control on adoption of self-service technology innovations, Journal of Services Marketing, vol. 16, pp. 553-572, 2002.
[18] J. Leyden, Florida man sues bank over $90K wire fraud, vol. 2006: The Register, 2005.
[19] C. Liu, J. T. Marchewka, J. Lu, and C.-S. Yu, Beyond concern: a privacy-trust-behavioral intention model of electronic commerce, Information & Management, vol. 42, pp. 127-142, 2004.
[20] N. Luhmann, Familiarity, confidence, trust: problems and alternatives, in Trust: Making and Breaking Cooperative Relations, D. Gambetta, Ed. New York: Basil Blackwell, 1988, pp. 94-107.
[21] A. McCullagh and W. Caelli, Who goes there? Internet banking: A matter of risk and reward, presented at ACISP 2005, Brisbane, 2005.
[22] J. M. Morse and L. Richards, Readme First for a User's Guide to Qualitative Methods. Thousand Oaks, Calif.: Sage Publications, 2002.
[23] J. S. Olson, J. Grudin, and E. Horvitz, A study of preferences for sharing and privacy, presented at CHI '05 extended abstracts on Human factors in computing systems, Portland, OR, USA, 2005.
[24] L. Palen and P. Dourish, Unpacking "privacy" for a networked world, presented at Proceedings of the conference on Human factors in computing systems, Ft. Lauderdale, Florida, USA, 2003.
[25] Princeton Survey Research Associates International, Leap of Faith: Using the Internet despite the Dangers Results of a National Survey of Internet Users for Consumer Reports WebWatch, Consumer Reports WebWatch, New York October 26 2005.
[26] M. A. Sasse and I. Flechais, Usable security: Why do we need it? How do we get it?, in Security and Usability: Designing Secure Systems that People Can Use, L. F. Cranor and S. Garfinkel, Eds. Sebastopol, CA: O'Reilly, 2005, pp. 13-30.
[27] B. Schneier, Applied Cryptography, Second ed. New York: John Wiley & Sons, 1996.
[28] B. Schneier, Secrets and lies: Digital security in a networked world. New York: John Wiley & Sons, 2000.
[29] S. Singh and K. Cassar-Bartolo, The privacy of money and health, presented at OZCHI, Wollongong, 2004.
[30] S. Singh and C. Slegers, Trust and electronic money, Centre for International Research on Communication and Information Technologies, Melbourne 1997 1997.
[31] H. Sraeel. (2005, April) Lopez v. B of A: Bad press or precedent setting?, US Banker [Online]. Available: http://www.us-banker.com/article.html?id=20050401HUQ7QVJB
[32] B. Suh and I. Han, Effect of trust on customer acceptance of Internet banking, Electronic Commerce Research and Applications, vol. 1, pp. 247-263, 2002.
[33]B. Tognazzini, Design for usability, in Security and Usability: Designing Secure Systems that People Can Use, L. F. Cranor and S. Garfinkel, Eds. Sebastopol, CA: O'Reilly, 2005, pp. 31-46.