Consumer risk perceptions in e-commerce

Pita Jarupunphol and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX
Tel. (44) 01784 414125, (44) 01784 443423
P.Jarupunphol@rhul.ac.uk, C.Mitchell@rhul.ac.uk

Abstract

Jarupunphol and Mitchell (2001) point out that there is a mismatch between the level of actual and perceived risks (the “risk perception gap”) associated with Internet e-commerce. This perception gap appears to be seriously restricting the growth of business-to-consumer (B2C) e-commerce since it deters many potential e-commerce participants. Although the emergence of e-commerce provides many benefits to consumers, e.g. convenience, greater choice, lower prices, and more information, consumers still have serious security concerns. The aim of this paper is to analyse the factors associated with consumer risk perceptions for Internet shopping. In addition, this paper also suggests guidelines for e-commerce merchants, which can be used to address negative consumer perceptions of Internet e-commerce.

Keywords: Electronic commerce (E-commerce), Secure Sockets Layer (SSL), Secure Electronic Transaction (SET), Transport Layer Security (TLS), cryptography, digital certificates, risk perception gap, perceived risks.

Word count: 3,402 words, 9 pages

1 INTRODUCTION

The fact that breaches of Internet security are reported with great frequency means that there is a danger that potential users will be reluctant to engage in e-commerce because of fears about security. According to a recent CommerceNet report (Barriers to Electronic Commerce 2000), security and trust are the dominant issues of concern to consumers. These issues appear to be the main barriers to consumer involvement in e-commerce.

In the business-to-consumer (B2C) context, whether the public should trust e-commerce is questionable since all purchasing processes are performed through the Internet, and the consumer cannot see the merchant with whom they are dealing. In addition, since e-commerce provides an alternative method for value exchange over the Internet, it is inevitable that financial risk becomes an issue of concern to e-commerce consumers. In this paper, we focus on the financial risk associated with the online payment methods most commonly used by e-commerce consumers.

The findings in this paper are based on widely available information and questionnaires related to consumer risk perceptions in Internet e-commerce taken from several sources. No additional desk research was conducted by the authors.

2 OVERVIEW OF E-COMMERCE RISKS

In Internet e-commerce, there is a mismatch between perceived and genuine levels of risk, Jarupunphol and Mitchell (2001). The main purpose of this paper is to indicate how this mismatch may be addressed, and thereby consumer participation increased. This requires an understanding of what the perceived risks are, and in this section we give an overview of those risks of most concern to e-consumers. We concentrate on financial information security since this issue appears to be the dominant one in shaping consumer perceptions of risk.

Several payment methods are used in Internet e-commerce, including plastic (debit/credit) cards, electronic cash (e-cash), and electronic cheque (e-cheque), (Oppliger, 2000). The credit card is the most commonly used method of payment for e-commerce consumers (Treese, 1998). According to an Internet shopping habits survey conducted by Survey.Net (http://www.survey.net), 36.0% of Internet users purchase goods by transmitting their credit card number via a secure form; the percentages for other payment methods are significantly lower.

Given that the debit/credit card is the primary means for consumers to purchase products or services online, the possible compromise of credit card numbers is clearly a serious threat to the consumer. Credit card numbers can be compromised in two main ways.

- Data transmission – financial information may be stolen by an interceptor.

- Data storage – financial information may be compromised by an intruder hacking into an e-commerce merchant website.

In the next section we consider these risks, together with the security measures that can be used to address them, in more detail.

3 ONLINE CREDIT CARD INFORMATION RISKS – SECURITY ASSESSMENT

Describing the two main risks to the confidentiality of credit card information, together with the main security measures used to ameliorate these risks, is a necessary first step to understanding the factors associated with consumer perceptions of risk. Once the true nature of the perceived risks has been identified, steps can be taken to reduce these risks and thereby increase consumer confidence.

3.1 Data transmission security

During data transmission, information sent between a consumer and an e-commerce server is typically secured by protocols such as Secure Sockets Layer (SSL) and IETF's SSL-based Transport Layer Security (TLS) (Hassler, 2000). Despite concerns in the past over restrictions on the implementation of strong cryptography within widely used versions of TLS and SSL, for most users the level of cryptographic protection available for transmitted data confidentiality appears adequate. Figure 1 shows how SSL operates.

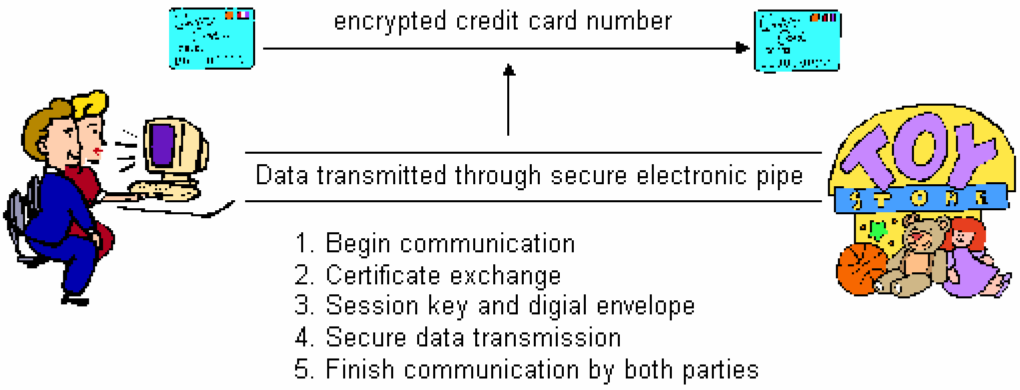
encrypted credit card number
Data transmitted through secure electronic pipe
1. Begin communication
2. Certificate exchange
3. Session key and digial envelope
4. Secure data transmission
5. Finish communication by both parties
TOY
STORE

Figure 1: SSL process in e-commerce transactions. Source: Oppliger (2000) and Rescorla (2001)

A different protocol called Secure Electronic Transaction (SET) is, according to Merkow (1998), arguably the only fully integrated protocol capable of securing an entire transaction. This scheme employs state of the art cryptographic techniques to protect the entire transaction process, including data transfers between merchant and consumer.

It would appear that as long as a scheme such as TLS or SET is employed, the risks to credit card information confidentiality arising from data transmission are low. However, as documented in Jarupunphol and Mitchell (2001), this analysis is not in accordance with consumer perceptions, a topic we explore again below.

3.2 E-commerce server security

A variety of countermeasures can be used to help protect e-commerce servers against attack by intruders, including firewalls and the adoption of detailed information security policies by network administrators. However there are also serious threats to such servers, and several cases of security breaches occurring at e-commerce websites have been reported, Power (2000, p.47). Poor configuration of servers and inadequate information security policies are likely to put at risk the confidentiality of stored consumer financial information, including credit card account details. We next consider in more detail how security vulnerabilities in merchant servers can arise.

3.2.1 Firewalls

Because of threats arising from connections made to port 80 (used by the HTTP protocol), which is used by web servers and always left open, a firewall is often used to protect a server against attacks by hackers, since it can analyse and capture the communication parameters of the traffic (Goncalves 2000). Furthermore, firewalls can also check the destination port and destination IP addresses of incoming Internet traffic. However, a firewall also needs to be properly configured in order to prevent malicious outsiders from compromising consumer financial information stored at the merchant web server. It is claimed by Power (2000, p.91) that “The encryption of a single transaction doesn't guarantee the confidentiality of the networked computer on which it is stored, just as a properly administered firewall doesn't ensure that there are no other points of entry into the network it guards”.

3.2.2 Server operating systems

There are a variety of operating systems (OSs) running on e-commerce servers including Linux, MacOS, Solaris, and Windows 2000 (NT). This means that there are also differences in terms of the security and vulnerability levels of these OSs. For example, configuration operations for UNIX and Windows 2000 (NT) are very different, and these OSs also require different e-commerce applications (Viega and Voas 2000).

If the operating system is poorly configured then information stored in the server may become vulnerable. Given the fact that modern OSs are extremely complex, experience shows that it is very difficult to remove all the accidental vulnerabilities from released versions, and poor configuration may simply mean failing to apply all the most recently available 'security patches' for the OS concerned. The merchant' s task is further complicated by the fact that, given that there are a number of different OSs in use, there is no single and widely disseminated process for configuring an e-commerce server OS.

3.2.3 Web server applications

In order to conduct e-commerce, it is necessary to install Web server applications on merchant servers. Examples of such applications include Apache, Cold Fusion, Microsoft (IIS), and Netscape Enterprise Server. These applications, however, may contain vulnerabilities that allow an attacker to compromise information stored in the server. According to a survey of Web server security conducted by Netcraft (http://www.netcraft.com/survey) between October 2000 and October 2001, 1 in 10 Microsoft IIS SSL e-commerce sites with encrypted transactions contain trapdoors allowing an attacker to monitor systems, and vulnerabilities were found in more than 20% of Microsoft IIS Web server applications.

3.2.4 Common gateway interface (CGI)

When a consumer PC transmits order and payment information entered on a form provided by an e-commerce website, CGI is working as an interface that transfers the user input to the server. However, this process is a further source of security vulnerabilities since it appears to be difficult to write 100% secure CGI scripts, (Schneier 2000). As argued by Bernstein et al. (1996), CGI is a major source of security problems in web servers, which may allow intruders to execute unauthorised commands or to discover information about the system.

4 CONSUMER RISK PERCEPTIONS

Human perceptions of e-commerce risks vary widely, just like other human characteristics. Some people believe that e-commerce is worth participating in because it offers several useful functions, such as convenience. On the other hand, others perceive e-commerce as being too risky. Although it has been reported by Visa and MasterCard in eMarketer (http://www.emarketer.com) of November 2000 that the online credit card fraud rate is relatively low, a survey conducted by the National Consumer Council (http://www.ncc.org.uk), summarised in Table 1, illustrates that most people believe that e-commerce is the riskiest shopping method in comparison with other traditional shopping methods, such as shopping over the telephone and using catalogues.

Table 1: Consumer attitudes to Internet shopping and other shopping methods. Source: NCC/MORI, April 2000. Participants: all (1,950), Internet users (513)

Methods of payment	Percentage of consumers believing this to be the riskiest payment method
E-commerce	35%
Telephone shopping	22%
Mail order from adverts	15%
Mail order from catalogues	5%
Digital TV	4%

High St/Shopping Centre	3%
Catalogue agent visiting	2%
N/A	14%

Table 1 shows that consumers do not trust online shopping, while offline shopping (e.g. at shopping centres) is perceived by consumers as the safest shopping method. A survey of 9,000 online users conducted by Bellman et al. (1999) further demonstrates consumer fears, in that more than 4,368 (42.9%) claimed to have never bought products or services online. This finding is consistent with the statistics from a survey conducted by Survey.Net (http://www.survey.net) that 34% of online users have never bought anything online.

Security of data transmission is arguably the issue of greatest concern to e-consumers. Consumers are particularly concerned that their credit card numbers will be stolen online during data transmission, Jarupunphol and Mitchell (2001).

5 ANALYSIS OF FACTORS ASSOCIATED WITH THE ADOPTION OF E-COMMERCE

We need to know why consumers perceive e-commerce to be the riskiest method of payment and why consumers do not trust security protocols to secure their financial information during transmission. Hoffman et al. (1999, pp.80-81) state that part of “the consumer lack of trust arises from the fact that cyberconsumers feel they lack control over the access that Web merchants have to their personal information during the online navigation process… consumers may fear typing in credit card information to any commercial Web provider”. As a consequence, consumers not only have negative perceptions about the nature of Internet shopping, but also misunderstand the real nature of security breaches in e-commerce. We now focus on the factors associated with consumer risk perceptions in more detail.

5.1 Personality

As mentioned before, human nature varies widely; some consumers may be inclined to use new technology, whereas others may prefer to continue doing their tasks in traditional ways. Similarly, consumer risk perceptions of Internet shopping also varies. This is supported by Bhatnagar et al. (2000) who argue that different individuals have different levels of risk acceptance.

5.2 Membership of a social system

Where the true levels of risk are unclear to users, e.g. in the context of non face-to-face shopping, recommendations from other members of a social system, such as friends, relatives, and neighbors, have an important effect on consumer participation, (Murray, 2000).

This is supported by Rogers (1983, p.5), who argues that information about an innovation “is communicated through certain channels over time among the members of a social system”. Prior to their adoption of Internet e-commerce, consumers may learn of its advantages and disadvantages via social interactions, e.g. with friends. Reports on television, newspapers and other mass media also play an important role in user adoption of e-commerce, since this is likely to be the prime source of information regarding security breaches for the majority of domestic users. As argued by Rosenbloom (2000), how the media interprets a social experience influences individual trust.

5.3 Knowledge

As previously mentioned, consumers are concerned that their credit card numbers may be compromised during data transmission. In reality, the majority of reported cases of Internet credit card fraud arise from weaknesses in merchant web servers, (Caldwell, 2000), (Tomlinson, 2000). In addition, consumers perceive e-commerce as the riskiest shopping method, whereas in fact the online transaction fraud rate appears to be lower than the rate for offline transactions (NOIE 2001). Furthermore, Jarupunphol and Mitchell (2001) and Tomlinson (2000) suggest that the likelihood of credit card theft during a web transaction may actually be less than the likelihood during an offline transaction. Thus it seems that the high risk perception for e-commerce at least partly derives from an inadequate understanding of Internet security technology by e-consumers.

5.4 Experience

In addition to knowledge, consumer experience is an important factor determining consumer perceptions of Internet shopping. It is important for consumers to at least try Internet commerce so that they can determine whether this shopping method is trustworthy. According to Bhatnagar et al. (2000, p.101), “the likelihood of purchasing on the Internet increases as the consumer's experience on the Internet increases”.

5.5 Shopping context

In traditional shopping, consumers can see the merchant with whom they are dealing. In addition, the consumer can be confident that the financial instrument, e.g. money or credit card number, is sent to the correct merchant during the payment process. Olson and Olson (2000) point out that face-to-face interaction is the foundation of trust in a number of activities. This probably explains why most consumers perceive the level of risk for traditional shopping methods to be relatively low.

In addition, since there is no face-to-face contact in e-commerce, Friedman et al (2000, p.39) state that it is difficult for users to “determine the potential for both financial harm and the good will of the organisation they are dealing with”. We can summarise the reasons for negative consumer perceptions of e-commerce as follows.

- Consumers are not confident that the merchant is trustworthy.
- Consumers will typically be more familiar with exchanging values by traditional - methods where buyer and purchaser can see each other.
- Consumers are not able to monitor what happens to their credit card numbers after they have submitted them to the merchant via their computer screens.
- Consumers do not understand the security technologies used to protect the confidentiality of consumer financial information.

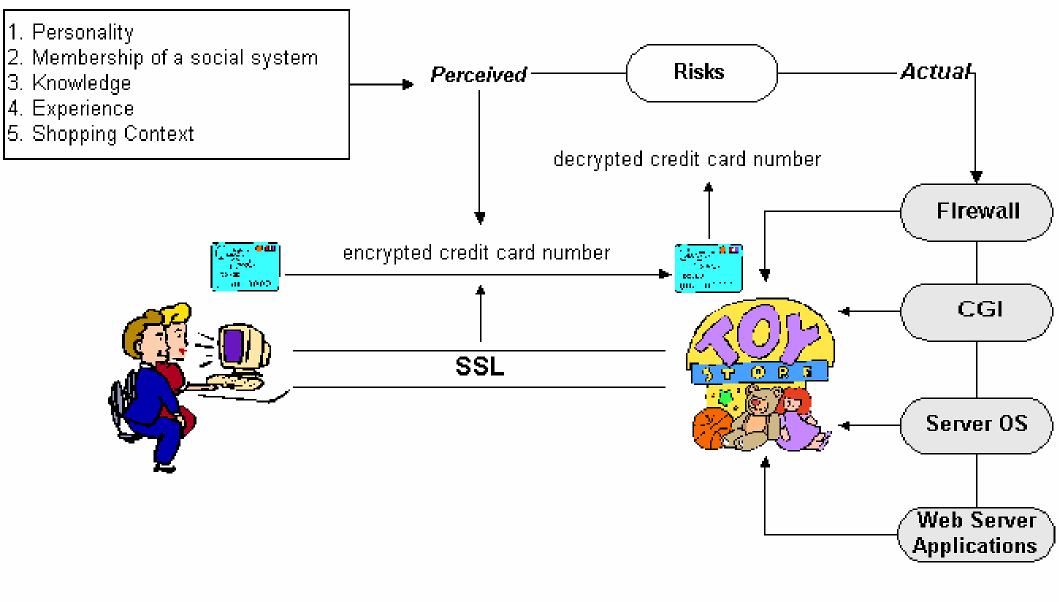

Figure 2: Consumer risk perception and actual risks in e-commerce

6 GUIDELINES

As previously described, consumer risk perceptions depend on several factors: personality, membership of a social system, knowledge, and shopping context. Consumers are widely informed about serious e-commerce security breaches by the mass media, and therefore it is important that e-commerce organisations address the actual threats to e-commerce sites lest bad publicity arising from a genuine security breach further damages e-commerce confidence.

One way in which consumer confidence can be increased at the same time as reducing the possibility of fraud is through the introduction of government or standards backed industry guidelines for e-commerce merchants, such as tScheme (http://www.tscheme.org), which is a not-for-profit organisation defining standards of good practice in order to provide assurance to individuals and organisations relying on electronic transactions. An example of this in a more general context is provided by BS 7799-1 = ISO/IEC 17799. Examples of possible guidelines for e-commerce merchants are as follows.

Guideline 1. Firewalls must be properly configured in order to hide internal network addresses from external users.

Guideline 2. CGI scripts must be carefully written to ensure that the hacker cannot take advantage of CGI vulnerabilities, and thereby gain access to an e-commerce site.

Guideline 3. Server OS and Web server applications must be carefully checked for backdoors or security holes that might allow an intruder to penetrate a server and steal consumer financial information.

Guideline 4. Consumer financial information must be stored in encrypted form. This will assure consumers that their information will remain private when stored at the merchant server.

Guideline 5. Cryptographically secure authentication techniques (e.g. based on digital signatures and public key certificates) must be deployed to protect e-commerce transactions. This may help to reduce consumer negative perceptions of Internet commerce since the consumer can authenticate the merchant.

Guideline 6. E-commerce web sites should be designed to educate and inform consumers about the security technologies used in e-commerce and the shopping navigation process. For example, web sites should invite participation by ensuring trust and accelerate action by clarifying responsibility, as suggested by Shneiderman (2000).

7 CONCLUSION

Many e-commerce merchant organisations employ security tools and techniques to address consumer fears regarding the security of online shopping. However, as previously described, this does not guarantee that more consumers will participate in e-commerce, since there are a number of different factors affecting consumer risk perceptions. An e-commerce trading organisation should consider all factors associated with consumer risk perceptions, since they are critical to the growth of e-commerce. In particular, security tools and techniques in themselves may not be sufficient to persuade consumers to participate in Internet shopping. What seems to be necessary is to have the means to convince e-consumers that their financial information will be protected throughout the e-commerce transaction lifecycle. The future of this research will focus on technologies addressing consumer risk perceptions in Internet e-commerce security.

References

Barriers to Electronic Commerce – 2000 Study (2000). Available at http://www.commercenet.com.

ISO/IEC 17799 (2000). *Information technology – Code of practice for information security management*.

Bellman, P., Lohse, J., and Johnson, E. J. (1999). **Predictors of online buying: Findings from the Wharton virtual test market**. *Communications of the ACM.* 42(12). 32-38.

Bernstein, T., Bhimani, A. B., Schultz, E., and Siegel, C. A. (1996). *Internet Security for Business*. John Wiley and Sons. New York.

Bhatnagar, A., Misra, S., and Rao, H. R. (2000). **On risk, convenience, and Internet shopping behaviour**. *Communications of the ACM*. 43(11). 98–106.

Caldwell, K. (2000). Global electronic commerce – moving forward. CommerceNet: The Public Policy Report. 2(11). 2-17.

Friedman, M., Kahn, P. H. and Howe, D. C. (2000). **Trust online**. *Communications of the ACM*. 43(12). 34-40.

Goncalves, M. (2000). *Firewalls – A Complete Guide*. McGraw-Hill. Berkeley.

Hassler, V. (2000). *Security Fundamentals for E-Commerce*. Artech House. Massachusetts.

Hoffman, D. L., Novak, T. P., and Peralta, M. A. (1999). **Building consumer trust online**. *Communications of the ACM.* 42(4). 80-85.

Jarupunphol, P. and Mitchell, C. (2001). **Actual and perceived levels of risk in consumer e-commerce**. In *Proceedings of 2nd International We-B Conference*. November. Edith Cowan University Press. Perth. 207-216.

Merkow, M. S., Breithaupt, J., and Wheeler, K. L (1998). *Building SET Applications for Secure Transactions*. John Wiley and Sons. New York.

Murray, K. B. (1991). **A test of services marketing theory: Consumer information acquisition activities**. *Journal of Marketing*. (55). 10-25.

The National Office for the Information Economy (NOIE) (2001). *Setting the record straight about online credit card fraud for consumers*. Available at http://www.noie.gov.au/publications/NOIE/consumer/creditcardfraud.pdf. Last access 7 November 2001.

Olson, J. S. and Olson, G. M. (2000). **i2i trust in e-commerce**. *Communications of the ACM*. 43(12). 41-44.

Oppliger, R. (2000). *Security Technologies for the World Wide Web*. Artech House. Massachusetts.

Power, R. (2000). *Tangled Web*. Que Corporation. Indiana.

Rescorla, E. (2001). *SSL and TLS --- Designing and Building Secure Systems*. Addison-Wesley. Boston.

Roger, E. (1983). *Diffusion of Innovation*. The Free Press. New York. 3rd Edition.

Rosenbloom, A. (2000). **Trusting technology**. *Communications of the ACM*. 43(12). 31-32.

Schneier, B. (2000). *Secrets and Lies*. John Wiley and Sons. New York.

Shneiderman, B. (2000). **Designing trust into online experiences**. *Communications of the ACM*. 43(12). 57-59.

Tomlinson, M. (2000). **Tackling e-commerce security issues head on**. *Computer Fraud and Security*. 2000(11). 10-13.

Treese, G. W. and Stewart, L. C. (1998). *Designing Systems for Internet Commerce*. Addison-Wesley. Massachusetts.

Veiga, J. and Voas, J. (2000). **The pros and cons of unix and windows security policies**. *IT Professionals*. 2(5). 40-45.