Electronic Commerce Research, 4: 9–21 (2004)
© 2004 Kluwer Academic Publishers. Manufactured in the Netherlands.

Technologies for Trust in Electronic Commerce

MARY ANNE PATTON patton@onlinestrategy.com.au
Online Strategy Consulting, 15 Tracey Street Kenmore, QLD, Australia

AUDUN JØSANG ajosang@dstc.edu.au
Distributed Systems Technology Centre, Queensland University of Technology, Brisbane, QLD 4001, Australia

Abstract

Lack of consumer trust in e-commerce merchants, e-commerce technology, and the social, financial and legal infrastructures of the e-commerce environment, poses a major challenge to the large-scale uptake of business to consumer e-commerce. Most traditional cues for assessing trust in the physical world are not available online. This paper gives an overview of some of the work being done to devise alternative methods for assessing, communicating and establishing trust in this environment. Examples are drawn from a wide range of disciplines including human–computer interaction, usability, marketing, information technology, mathematics, linguistics and law. Industry, self-regulatory and government initiatives aimed at building consumer trust and confidence in e-commerce are also discussed.

Keywords: trust, privacy, security, e-commerce, reputation systems, payment intermediaries, trustmark seals, cryptography, digital certificates, mathematical trust models, embodied conversational agents, alternative dispute resolution mechanisms

1. Introduction

Trust is a catalyst for human cooperation. It allows people to interact spontaneously and helps the economy to operate smoothly. Lack of trust on the other hand is like sand in the social machinery. It makes us waste time and resources on protecting ourselves against possible harm and thereby clogs up the economy. Fukuyama [20] describes the role mutual trust plays in the formation of social structures. However distrust can also serve as a useful state of mind, as it enables us to avoid harm when confronted with unreliable systems or dishonest people and organisations.

Consumers perceive the Web as a world of chaos, offering both opportunities and threats [Cheskin Research & Studio Archetype/Sapient, 11]. Factors affecting trust in e-commerce for consumers include security risks, privacy issues, and lack of reliability in e-commerce processes in general. Studies and reports by consumer associations and government organisations show that some of these fears are well founded. A study by Consumers International [12] involved researchers from 11 countries placing 151 orders at sites in 17 countries. They found that 9% of goods ordered never arrived. In 20% of cases the amount actually charged was higher than expected, and there were problems obtaining a refund in 21% of purchases, despite the fact that the sites in question advertised that refunds were available. The US Federal Trade Commission reports a rapid rise in the number of online fraud and deception complaints from consumers. In 1997, fewer than 1000 complaints were received and in 2000 the number had increased to over 25 000 [US FTC, 32]. However it has been shown that media attention given to security risks and online fraud amplifies consumer fears, and concern about the security of credit card information in particular is seen by some to be irrationally exaggerated [Pichler, 29].

It is in this environment of risk and uncertainty that e-commerce merchants must develop strategies for establishing trustworthiness, and that systems should be developed to assist consumers in assessing the level of trust they should place in an e-commerce transaction. This paper presents a selection of technologies and strategies that we believe are valuable and have potential for further development.

Web interface elements, including trustmark seals, are discussed in terms of their effect on the perceived trustworthiness of web sites. Anonymisers, payment intermediaries, insurance providers and alternative dispute resolution systems, are discussed as mechanisms that may enhance system trust [McKnight and Chervany, 24], increasing the likelihood that a consumer will engage in an e-commerce transaction due to their trust in the e-commerce infrastructure, regardless of whether or not they trust the online merchant. Reputation systems, mathematical trust models and to some degree, trustmark seals and the W3C's Platform for Privacy Preferences project, are discussed in terms of their potential for assisting consumers to make more informed decisions about the trustworthiness of their e-commerce interactions. Security strategies are examined in terms of their crucial role in improving the actual trustworthiness of e-commerce interactions. Current work on Embodied Conversational Agents is highlighted as an area of research that may provide valuable clues for improving the e-commerce interfaces of the future.

2. The nature of trust and e-commerce transactions

Numerous models for the way trust is established and maintained in an e-commerce setting have been proposed. The Cheskin Research & Studio Archetype/Sapient eCommerce Trust Study [11] describes trust as a dynamic process that deepens or retreats as a function of experience. It states that once consumers have been provided with a sense of security, their focus changes to five signifiers of trust: brand, navigation, fulfilment, presentation and technology. Nielsen [27] points out that real trust builds through a company's actual behaviour towards its customers over time. Trust is seen to be difficult to build and easy to lose [Nielsen et al., 28].

Egger and de Groot's model of trust for e-commerce (MoTEC) [16] has four main components: factors affecting trust before the site is accessed, including brand reputation, previous off-line experiences with the merchant, and differences between individuals in their general propensity to trust; interface properties such as graphic design and layout, content organisation and usability; informational content including information the merchant provides about products and services, privacy policies, and privacy practices; and relationship management, including post-purchase communication and customer service.

Since trust is based on experience over time, establishing initial trust can be a major challenge to newcomers in e-commerce, particularly those who do not have well established off-line brands [Pichler, 29]. Without initial trust, merchants cannot build a good transaction history—and without a good transaction history, consumers may not build trust in these merchants. Pichler [29] describes how, to some extent, merchants can 'buy' trust though advertising: this evidence of financial investment implies to consumers that a firm will not engage in quick gain deception. However, a high entry barrier for new merchants, particularly for small and medium sized enterprises, will remain unless effective reliance mechanisms aimed at enhancing system trust are developed. This paper outlines a number of new and emerging consumer reliance mechanisms.

Pichler [29] also describes e-commerce transactions as distance transactions that have much in common with mail order catalogues and telephone orders. Distance transactions often provide insufficient information about the merchant and about the goods and services offered. He highlights the fact that they also require consumers to accept the 'risk of prior performance,' which can leave them in a vulnerable position [Pichler, 29]. The consumer generally has no opportunity to see and feel products, or to evaluate a service in detail before making a purchase decision. Information about the physical location of a merchant is often missing, as are the body language and gestures of customer service staff [Pichler, 29]. The information deficiencies inherent in distance transactions provide valuable clues for developing strategies to communicate trustworthiness through the Web interface and to generate confidence in the e-commerce experience.

3. Communicating trustworthiness through the Web interface

A number of researchers have investigated Web interface properties in terms of the effect they have on perceived trustworthiness. Fogg et al.'s quantitative study [17] identified the extent to which 51 Web elements affected peoples' perceptions of credibility. From these results they describe seven guidelines for creating highly credible Web sites. They suggest designing Web sites to convey the 'real world' aspect of the organisation by, for example, including physical address details and high quality photographs of employees; making Web sites easy to use; including evidence of expertise, for example, by listing an author's qualifications; communicating the honest, unbiased nature of the Web site, for example, by linking to outside sources; tailoring the experience for the user; avoiding amateur design glitches such as typographical errors and broken links; and avoiding overly commercial elements, such as making advertisements difficult for users to differentiate from content (results indicate that this practice reduces perceived credibility more than any other factor included in the study).

A further study by Fogg et al. [18] found that banner ads with low reputability had a much greater destructive effect on the credibility of Web content than banner ads with high reputability, and suggests that high quality author photographs will increase credibility more than author bylines.

The Nielsen Norman Group's E-commerce User Experience study [Nielsen et al., 28] also makes recommendations for communicating trustworthiness. These include providing: company information that is easy to find; pricing, including taxes and shipping costs, early in the interaction; balanced information about products; professional Web site design with human error messages; clear and friendly privacy, security and return policies; appropriate requests for personal information and clear explanations for why information is being sought; alternative methods of ordering; and access to helpful people through email or live chat.

The Cheskin/Sapient study [11] states that effective navigation is necessary for communicating trust in e-commerce Web sites, and that quality of navigation is used as a measure by consumers to judge how well a site is likely to meet their needs. The study also examines the importance of brand and the role that seals of approval play in enhancing perceived trustworthiness.

4. Privacy strategies

Public surveys indicate that privacy is the major concern for people using the Internet [Cavoukian and Crompton, 9]. Privacy related complaints that are made to the US Federal Trade Commission include complaints about unsolicited email, identity theft, harassing phone calls, and selling of data to third parties [Mithal, 26].

One attempt to address privacy concerns and thereby increase user trust in the Web is the W3C's Platform for Privacy Preferences (P3P) Project [Cranor et al., 13]. P3P enables Web sites to express their privacy practices in a standardised, XML-based, format that can be automatically interpreted by user agents such as a Web browser. The aim is that discrepancies between a site's practices and the user's preferences can be automatically flagged. While it is difficult to predict how widely the P3P specification will be adopted by e-commerce Web sites, it is interesting to note that the recently released version (V6.0) of Microsoft's Internet Explorer is P3P enabled [Benner, 4]. Nine aspects of online privacy are covered by P3P, including five that cover data being tracked by the site: who is collecting the data; what information is being collected; for what purposes is it being collected; which information is being shared with others; and who are the data recipients. Four topics explain the site's internal privacy policies: can users make changes in how their data is used; how are disputes resolved; what is the policy for retaining data; and where can the detailed policies be found in a 'human readable' form.

P3P is unable to guarantee or enforce the privacy claims made by Web sites. However, the W3C states that future versions of P3P may incorporate XML signatures to allow for non-repudiation of agreements between users and Web sites. Future versions may also incorporate a mechanism to allow user agents to negotiate and transfer user data. Despite its potential, detractors say that P3P does not go far enough to protect privacy. They believe that the aim of privacy technology should be to enable people to transact anonymously [Dutton, 15].

Private privacy service providers or *anonymisers* are emerging [The Economist, 31]. One example is iPrivacy, a New York based company that professes on its Web site, "not even iPrivacy will know the true identity of the people who use its service." To utilise the technology, users first download software from the Web site of a company they trust, for example a bank or credit card company. When they wish to purchase a product online, they use the software to generate a one-off fictitious identity (name, address and email address). Users are given the choice of collecting the goods from their local post office (their post or zip code is the only part of the address which is correct) or having the goods delivered by a delivery company or postal service that has been sent a decoded address label. Originally the iPrivacy software generated a one-off credit card number for each transaction. The credit card issuer matched the credit card number it received from the merchant with the user's real credit card number and then authorised payment. However, this proved to be a major job for banks to integrate and is no longer offered by iPrivacy. There are still other companies such as Orbiscom and Cyota that do offer one-off credit card numbers, but these have captured limited use to date.

Another type of privacy provider or *infomediary* is emerging which sells aggregated buyer data to marketers, but keeps individual identifying information private [The Economist, 31]. One example of this is Lumeria, a Berkley based company that provides royalties to people who participate. In the Lumeria system, users download free software that encrypts their profile and stores it on Lumeria's servers. The user accesses the Web via a Lumeria proxy server, which shields their identity from merchants and marketing companies whilst enabling marketing material that matches their profile to be sent to them.

To be maximally effective, technological and self-regulatory privacy solutions need to operate within adequate legislative frameworks. However, the major driver of e-commerce, the US, does not have rigorous mandatory privacy protection legislation in place [Cavoukian and Crompton, 9]. Consumer protection in the global e-commerce environment will remain a challenge while there is so much variation in privacy legislation between countries.

5. Self-regulation and trustmark seals

A number of Trustmark seals have been developed to provide assurances about Web business practices and policies through the Web interface. One example is TRUSTe, which audits a site's stated privacy policies and allows sites to display the TRUSTe seal if privacy policies and disclosure meet specific standards. BBBOnline has a similar privacy seal and also offers an online reliability program that incorporates a dispute resolution mechanism. The CPA WebTrust seal was developed by accounting organisations in Canada and the US. It originally certified sites' stated privacy, security, and business practices including order processing, shipping times, and return policies. Despite attempts by accounting professionals to introduce the WebTrust seal to Australia, it has not been widely adopted. The e-commerce market in Australia is relatively small, and businesses reported that the seal was too inflexible for their needs. To meet market demand, most of the large accounting firms now offer merchants the option of individual modules of online assurance as an alternative. The most popular modules are security and privacy. Firms provide an online report in conjunction with their seal, and as with CPA WebTrust, the site is re-audited every ninety days. Cheskin/Sapient's US study [11] found that where trustmark seals were recognised, they increased consumer perceptions of a site's trustworthiness. Although it is not a trustmark seal, the VeriSign logo was recognised by one third of respondents. Of these, over one-half claimed it would increase their trust in a Web site. This is due to transference of trust from the seal to the merchant. A later study [Cheskin Research, 10] found that there was little increase in trust through trustmark seals in Latin America and

Brazil, where the seals were largely unrecognised. As with P3P, the seals generally do not guarantee that e-commerce merchants' stated policies reflect their actual practices. The seal providers themselves are not subject to independent objective monitoring and remain more advocates for industry than for consumers [Cavoukian and Crompton, 9].

6. Security strategies

The great Internet innovation that has led to the e-commerce revolution over the past decade has been the result of an open and flexible network environment with ever increasing connectivity and functionality. Unfortunately this has also created many security vulnerabilities which represent a threat to users of the Internet and to e-commerce merchants. It is commonly accepted that people will only trust and embrace e-commerce if they perceive that sufficient security is in place, and considerable effort is therefore being put into the development and deployment of security services. What is often ignored is that there is a trade-off between functionality and security. The e-commerce industry is driven by functionality, and therefore security is often seen as an obstacle to e-commerce innovation [Fontana, 19]. The current insecurity of commercial systems is thus perfectly rational from the economists' viewpoint, however undesirable from the users' [Andersen, 2, p. 519]. In order to satisfy the need to build trust on one hand, and to support innovation on the other, there is a danger that the e-commerce industry will promote 'perceived' security rather than ensuring 'real' security.

Important requirements for e-commerce security are the need to protect sensitive information that is stored on computers before and after an e-commerce transaction, to verify the identity of the other party in the transaction, to ensure that no one can intercept the information being exchanged during the transaction, and in general to prevent disruption of services and applications. Satisfying only one of these requirements in isolation (like, e.g., communication security without system security) often has limited value because the overall level of security can not be stronger than the weakest link. The security expert Gene Spafford has illustrated this by saying: "Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit-card information from someone living in a cardboard box to someone living on a park bench."

Although data transmitted on the Internet can be intercepted, researchers maintain that cryptographic communication security is adequate, when used correctly, to protect against "all but the most highly motivated criminal interceptor" [Dutton, 15]. The importance of system security is best illustrated by the fact that almost all reported attacks are targeted against e-commerce servers. System security can be addressed by installing firewalls and intrusion detection systems, by monitoring security alerts and prompt implementation of security patches. However this requires skilled system administrators to continuously look after systems, which is relatively labour intensive.

The issues of authenticating the identity of remote transaction partners and non-repudiation of transactions can theoretically be solved by public-key cryptography. It is predicted that every organisation and individual on the Internet will have their own public/private key pair, which will form the basis of their digital identity. This requires the secure generation and distribution of potentially hundreds of millions of key pairs which poses formidable key and trust management challenges. Private keys must be kept secret by their owners. Public keys are stored in public directories and distributed in the form of public-key certificates, which are signed by Certification Authorities (CAs), to ensure their authenticity. CAs must be trusted to do thorough key owner identification and key owners must be trusted to keep their private keys secure. But what if a CA issues a certificate without properly checking owner's identity? This already happened when VeriSign, the worlds largest CA, issued false certificates in the name of Microsoft, because it failed to correctly identify the owners [Microsoft, 25]. What if a private key is stolen or leaked to the public by accident, or intent? Private keys are often stored on Web servers, and because Web servers are often successfully attacked, these keys are vulnerable to theft and misuse. Such events could lead to systems and users making incorrect assumptions about identities, especially as current Web browsers are not enabled to access Certificate Revocation Lists.

Human factors and user interface issues pose a major challenge to information security today. Otherwise secure systems are regularly defeated by simple social engineering [Andersen, 2 p. 37; Lemos, 22], and e-commerce systems need to be designed to be as robust as possible against such attacks. One of the few published research papers to deal empirically with user interface issues in security is "Why Johnny can't Encrypt: A Usability Evaluation of PGP 5.0" [Whitten and Tygar, 34]. PGP [Zimmermann, 36] is regarded as having a good user interface by general standards. However the researchers concluded that PGP 5.0 was inadequate in terms of usability to provide effective security for most computer users. They argued that a different usability standard is required for security, and that current software interface design techniques are not appropriate to security [Whitten and Tygar, 34]. Given that most security failures are caused by human error, increased emphasis on human factors in security is required.

7. Mathematical trust models

Research in formal trust models has mostly taken place within the information security community. Trust models defined by, e.g., PGP [Zimmermann, 36], Maurer [23], Abdul-Rahman and Hailes [1], and Jøsang [21], mainly address the problem of trusting an entity's identity by using cryptographic mechanisms for propagating trust measures. These models may also be used to derive trust in entities themselves, and thereby provide a similar type of evidence to reputation systems.

People tend to have difficulties in determining the numerical trust measures that are needed as input. One approach to this problem is to use a discrete set of verbal tags as input, such as *strong trust*, *weak trust*, *uncertain trust*, *weak distrust*, and *strong distrust*, and to either let the system work directly with these (as in PGP) or translate them into numerical values. The trust models aim to make the derivation of trust measures both intuitive and mathematically sound. The goal is to develop systems that in an automatic fashion are able to reason about trust in a similar way to humans while at the same time being robust against manipulation and avoiding typical human reasoning fallacies. Practical implementation and empirical testing is needed to determine the suitability of this approach.

8. Payment intermediaries and insurance providers

A payment intermediary is often the only party in an e-commerce transaction that is able to verify the merchant's identity and location [Pichler, 29]. Pichler [29] claims that credit card companies are in an influential position because of this. Because merchants rely on them for payment, they are in a position to sever services to fraudulent merchants. He advocates expanding their role, and sees opportunities for the development of new types of payment intermediaries as a means of increasing consumer confidence in e-commerce. Payment intermediaries can assist consumers by alleviating the 'risk of prior performance,' which typically leaves the consumer in a vulnerable position in online transactions [Pichler, 29]. Payment intermediaries can also help new merchants overcome the problem of establishing initial trust.

Escrow services are one form of payment intermediary currently used in B2C, C2C, and B2B e-commerce. They hold payments from the buyer until the buyer has received and accepted the goods, at which point payment is made to the seller. New types of credit cards are also emerging, which offer consumers online shopping guarantees. For example 'Amex Blue' offers to refund the price of goods if a customer is unhappy with them, regardless of whether the Internet merchant has a refund policy. There is a $300 refund limit per item and a $1000 refund limit per year. Insurance companies are also emerging to provide insurance for e-commerce transactions. For example a German insurance company, Gerling, offers insurance and provides a 'trusted shop' seal to participating e-commerce sites [Pichler, 29].

9. Reputation systems

Reputation systems have also emerged as a method for fostering trust amongst strangers in e-commerce environments. A reputation system gathers, distributes, and aggregates feedback about participants' behaviour. Resnick et al. [30] state that these mechanisms can help people make decisions about who to trust and provide an incentive for honest behaviour. They may also have some influence on deterring dishonest parties from participating.

Past experience with a remote transaction partner is projected into the future, giving a measure of their trustworthiness. This effect has been called the 'shadow of the future' by political scientist Robert Axelrod [3]. Without such systems, where strangers are interacting in an e-commerce setting, the temptation to act deceptively for immediate gain could be more appealing than cooperation.

The first Web sites to introduce reputation schemes were on-line auction sites such as eBay. They are now also used by company reputation rating sites such as BizRate, which ranks merchants on the basis of customer ratings. Consumer Reports Online's eRatings, rates merchants on the basis of test purchases carried out by Consumer Reports staff. Product review sites have also emerged, such as Epinions.com, in which reviews themselves are actually rated by other reviewers. Except for eRatings, most of the systems do little to overcome the issue of establishing initial trust for new merchants in the e-commerce arena, as strong reputation ratings generally require time to develop [Pichler, 29].

In the physical world, capturing and distributing feedback can be costly. In comparison, the Internet is extremely efficient. However reputation systems still encounter significant challenges. Feedback can get erased if an entity changes its name, and a dishonest participant can use this to start fresh every time it builds up a bad reputation. People may not bother to provide feedback at all, negative feedback can be difficult to elicit, and it is difficult to ensure that feedback is honest [Resnick et al., 30]. One example of dishonesty through reputation systems is the attempt by three men to sell a fake painting on eBay for $US135,805 [Young, 35]. The sale was abandoned just prior to purchase when the buyer became suspicious. It was shown that two of the fraudsters actually had good Feedback Forum ratings, developed through rating each other favourably, and by engaging in honest sales prior to the fraudulent attempt. It emerges that reputation systems have a multitude of complex facets, and their study is becoming a fertile ground for research[1].

10. Humanoids

Linguistics researchers, who have an understanding of the way trust is built through conversational rituals, are working with information technology researchers, to create computer-generated agents in a human-like form, with the ability to engage in social dialogue. They use gesture, gaze, posture, intonation and other elements, to emulate the experience of human face-to-face interaction. Researchers at MIT's Media Lab [Bickmore and Cassell, 6] have developed prototypes called Embodied Conversational Agents (ECAs). One of their prototypes is designed specifically for the e-commerce domain of real estate. Other studies on conversational agents have been done by, e.g., Beskow and McGlashan [5], and Van Mulken et al. [33].

Bickmore and Cassell's prototype, REA, or Real Estate Agent [6], is able to engage in small talk and monitor feedback from its conversational partner. It is able to keep track of conversational topics and execute conversational manoeuvres, such as guiding a conversation from general talk about the weather, to talk about the weather in Boston, to a conversation about real estate prices in Boston. Conversations are only permitted to move to more sensitive task talk, such as the size of home or price range being sought, once a predefined solidarity rating for that topic has been reached. In one experiment, participants are shown two virtual apartments and either engage in a conversation with small talk leading to task talk, or with task talk alone. They complete a questionnaire that includes measures of perceived competence, likeability, intelligence, and a standard measure of trustworthiness. Results so far indicate that many users find the agent more competent, reliable, and knowledgeable when it uses small talk than when it engages only in task talk [Bickmore and Cassell, 6].

11. Alternative dispute resolution

Alternative dispute resolution mechanisms (ADRs) are also being explored as a means of improving trust and confidence. The assumption is that the uptake of e-commerce by consumers will increase if people feel confident that they will have recourse to a fair, reliable and effective process, if a dispute arises that is not able to be sufficiently resolved by the business's own customer relations processes.

While ADR stakeholders agree that both merchants and consumers should have access to the legal system at all times, the legal system is seen as inappropriate for many e-commerce disputes [Carblanc, 8]. Problems include substantial legal costs, which often outweigh the value of the items in dispute, and the fact that the court process can be lengthy. It can also be difficult to determine which law applies to e-commerce disputes, which authority has jurisdiction over a dispute, and whether or not the decision is enforceable across borders. ADR provides a solution to many of these issues. Generally the ADR process begins when a party files a complaint with an ADR provider who then notifies the other party or parties that a complaint has been made. Next, a series of interactions occur between the parties with the intervention of the neutral third party, as they attempt to come to a resolution. ADR can be human-assisted or fully automated. It can vary from assisted negotiation, in which a third party guides the disputing parties to a mutual decision, to arbitration, where facts are handed over to a third party who makes the final decision.

More than 39 online ADR systems have been identified [Carblanc, 8]. Generally agreed upon principles for ADR are that it should be accessible, timely, neutral, voluntary, free or cheap for consumers, and transparent in terms of its practices, costs, and types of disputes handled. The Trans-Atlantic Consumer Dialogue, a forum of US and EU consumer organisations, suggests that an international online clearinghouse for publishing details of all ADR cases should be established, which would be accessible to law enforcement agencies and the public [Carblanc, 8]. The Global Business Dialogue on Electronic Commerce, an international group of chief executive officers, has stressed that while governments should encourage the uptake of ADR programs by industry, they should avoid establishing mandatory accreditation schemes for ADR providers [Carblanc, 8]. However, although they have not established mandatory schemes, countries such as the United Kingdom have established umbrella schemes (e.g., TrustUK), that endorse trustmark programs only if they provide acceptable ADR mechanisms and meet particular standards [Bond, 7].

It has been suggested that businesses that take part in ADR, should have links from their Web sites to one or more ADR providers, stating clearly that if a customer is not completely satisfied, they have recourse to the ADR system. Governments, consumer organisations, and trade associations could also provide links from their Web sites to ADRs to make it easy for consumers to find help [Carblanc, 8].

One of the major challenges for ADR involves the enforceability of decisions. An extremely controversial issue, even within groups of stakeholders, is determining whether, or under what conditions, an ADR arbitration decision should be binding on one or more parties [Dorskind, 14]. It has been suggested that, if ADR systems are operated by trade associations or other industry groups, compliance with decisions should be a requirement for maintaining membership. Others who facilitate merchant sales, for example, online auction sites and payment intermediaries, would be encouraged to deny services to a merchant that did not abide by ADR decisions [Carblanc, 8].

12. Future work

Trust issues and their effects on e-commerce uptake provide a rich and compelling impetus for further work. While trust is seen as an important issue in online buying behaviour, more work needs to be done to determine how trust interacts with other factors, including consumer motivation. It would be valuable to look at how strategies for communicating trust and credibility through the Web interface might be tailored for different types of industries, professions and businesses, and to describe and measure the actual effects on buyer behaviour and sales, when various trust communicating strategies are implemented. Fine-tuning and strengthening of privacy protection legislation for the online environment is required in many countries, to ensure that technological and self-regulatory privacy solutions are maximally effective and enforceable. Future versions of P3P may go some way towards more enforceable privacy if digital signatures are included in the specification to provide non-repudiation. Research into practical applications of mathematical trust models may provide the basis for tools to help consumers make trust decisions in e-commerce. Further research into trust-building conversation rituals and fine-tuning the conversational abilities of Embodied Conversational Agents, may result in improved e-commerce Web interfaces, and may provide a ‘human’ touch that improves usability. While communication security is relatively easy to implement, work is required to make it more simple for e-commerce participants to achieve strong system security. Since the majority of security failures occur through human error, it would be valuable to conduct more research into security management practices, usability issues in security, and improving security user interfaces. As discussed, work is currently being carried out to improve the metrics used in reputation systems. More work is needed to devise ways of protecting these systems from manipulation by dishonest participants. If alternative dispute resolution mechanisms are to provide increased trust in global e-commerce, further work is needed to determine how effective these mechanisms actually are within different cultures, and to utilise emerging technologies, such as voice recognition and translation technology in multilingual disputes. It will also be valuable to study new trust-building solutions as they emerge in the private sector. Solutions to privacy concerns are already emerging, and it will be interesting to see whether new types of payment and insurance solutions tailored to the e-commerce environment become widely adopted.

13. Conclusion

Without the ability to trust we hesitate. Consumer reluctance to engage in e-commerce is partly due to a lack of trust in e-commerce merchants, e-commerce technology and business processes, and the lack of reliable, enforceable systems to provide redress should things go wrong. This paper has reviewed a wide range of technologies and strategies that attempt to overcome these problems, and has presented some suggestions for future research that will hopefully result in improved trust assessment tools for consumers, and increased consumer confidence in e-commerce as a whole.

Acknowledgments

The work reported in this paper has been funded in part by the Co-operative Research Centre for Enterprise Distributed Systems Technology (DSTC) through the Australian Federal Government's CRC Programme (Department of Industry, Science & Resources).

Note

1. The Reputations Research Network is a forum for people conducting research into how reputation systems should work in theory, how they actually work in practice, and how they could work better (`http://databases.si.umich.edu/reputations/`).

References

[1] Abdul-Rahman, A. and S. Hailes. (1997). "A Distributed Trust Model." In *Proceedings of the 1997 New Security Paradigms Workshop*. ACM, pp. 48–60.

[2] Andersen, R. (2001). *Security Engineering*. Wiley.

[3] Axelrod, R. (1984). *The Evolution of Cooperation*. New York: Basic Books.

[4] Benner, J. (2001). "MS Gets Privacy-Happy With New IE." *Wired News*, `http://www.wired.com/news/privacy/0,1848,43686,00.html`.

[5] Beskow, J. and S. McGlashan. (1997). "Olga: A Conversational Agent with Gestures." In *Proceedings of the IJCAI'97 Workshop on Animated Interface Agents: Making Them Intelligent*, Nagoya, Japan.

[6] Bickmore, T. and J. Cassell. (2001). "Relational Agents: A Model and Implementation of Building User Trust." In *CHI 2001 Conference Proceedings*. ACM Press.

[7] Bond, M. (2000). "Role of Stakeholders in Identifying Essential Elements of Trustmark Programs, Codes of Conduct and Dispute Resolution Schemes." In *Proceedings of the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to Consumer Dispute Resolution*, The Hague, `http://www.oecd.org/dsti/sti/it/secur/act/online_trust/presentations.htm`.

[8] Carblanc, A. (2000). "Privacy Protection and Redress in the Online Environment: Fostering Effective Alternative Dispute Resolution." In *Proceedings of the 22nd International Conference on Privacy and Personal Data Protection*.

[9] Cavoukian, A. and M. Crompton. (2000). "Web Seals: A Review of Online Privacy Programs." A Joint Project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, `http://www.ipc.on.ca/english/pubpres/papers/seals.pdf`.

[10] Cheskin Research. (2000). *Trust in the Wired Americas*. Cheskin Research, `http://www.cheskin.com/think/studies/trust2.html`.

[11] Cheskin Research & Studio Archetype/Sapient. (1999). *eCommerce Trust Study*. Sapient, `http://www.sapient.com/cheskin/`.

[12] Consumers International. (1999). *Consumers@shopping: An International Comparative Study of Electronic Commerce*. Consumers International's Programme for Developed Economies and Economies in Transition, `http://www.consumersinternational.org/campaigns/electronic/e-comm.html`.

[13] Cranor, L. et al. (2002). *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C Recommendation 16 April 2002, `http://www.w3.org/TR/P3P/`.

[14] Dorskind, J. (2000). "Remarks to ADR by the US Department of Commerce." In *Proc. of the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to*

Consumer Dispute Resolution, The Hague, http://www.oecd.org/dsti/sti/it/secur/act/online_trust/presentations.htm.

[15] Dutton, P. (2000). "Trust Issues in E-Commerce." In *Proceedings of the 6th Australasian Women in Computing Workshop*, Griffith University, pp. 15–26.

[16] Egger, F. and B. de Groot. (2000). "Developing a Model of Trust for Electronic Commerce: An Application to a Permissive Marketing Web Site." In *Proceedings of the 9th International World-Wide Web Conference*, Foretec Seminars.

[17] Fogg, B. et al. (2001a). "What Makes Web Sites Credible? A Report on a Large Quantitave Study." In *Proceedings of CHI 2001*. ACM Press, pp. 61–68.

[18] Fogg, B. et al. (2001b). "Web Credibility Research: A Method for Online Experiments and Early Study Results." In *Proceedings of CHI 2001*. ACM Press, pp. 295–296.

[19] Fontana, J. (2000). "Outlook Patch Called Overkill." *CNN.com NewsNet*, http://www.cnn.com/2000/TECH/computing/05/23/outlook.overkill.idg/.

[20] Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*. New York: The Free Press.

[21] Jøsang, A. (1999). "An Algebra for Assessing Trust in Certification Chains." In J. Kochmar (ed.), *Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99)*. The Internet Society.

[22] Lemos, R. (2000). "Mitnick Teaches 'Social Engineering."' *ZD Net News*, http://zdnet.com.com/2100-11-522261.html?legacy=zdnn.

[23] Maurer, U. (1996). "Modelling a Public-Key Infrastructure." In E. Bertino et al. (eds.), *Proceedings of the Fourth European Symposium on Research in Computer Security (ESORICS'96)*. Springer.

[24] McKnight, D. and N. Chervany. (1996). "The Meanings of Trust." Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Reseach Center, http://misrc.umn.edu/wpaper/.

[25] Microsoft. (2001). "Microsoft Security Bulletin MS01-017 (March 22, 2001): Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard." http://www.microsoft.com/technet/security/bulletin/MS01-017.asp.

[26] Mithal, M. (2000), "Illustrating B2C Complaints in the Online Environment." Presentation by the US Federal Trade Commission and Industry Canada, at the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to Consumer Dispute Resolution, The Hague, http://www1.oecd.org/dsti/sti/it/secur/act/online_trust/presentations.htm.

[27] Nielsen, J. (1999). "Trust or Bust: Communicating Trustworthiness in Web Design." Jakob Nielsen's Alertbox, http://www.useit.com/alertbox/990307.html.

[28] Nielsen, J., R. Molich, C. Snyder, and S. Farrell, (2000). "E-commerce User Experience." Technical report, Nielsen Norman Group.

[29] Pichler, R. (2000). *Trust and Reliance—Enforcement and Compliance: Enhancing Consumer Confidence in the Electronic Marketplace*. Stanford Law School, www.oecd.org/dsti/sti/it/secur/act/online_trust/Consumer_Confidence.pdf.

[30] Resnick, P. et al. (2000). "Reputation Systems." *Communications of the ACM* 43(12), 45–48.

[31] The Economist. (2000). "The Coming Backlash in Privacy." *The Economist Technology Quarterly*, December 9.

[32] US FTC. (2001). "Boom in E-Commerce Has Created Fertile Ground for Fraud." US Federal Trade Commission, http://www.ftc.gov/opa/2001/05/iftestimony.htm.

[33] Van Mulken, S., E. André, and J. Müller. (1999). "The Trustworthiness of Lifelike Interface Characters." In *Proceedings of the 8th International Conference on Human–Computer Interaction (HCI International'99)*, Munich, Germany.

[34] Whitten, A. and J. Tygar. (1999). "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In *Proceedings of the 8th USENIX Security Symposium*.

[35] Young, E. (2001). "Not a Pretty Picture." *The Industry Standard* (online newsletter), http://www.thestandard.com/article/0,1902,22875,00.html.

[36] Zimmermann, P. (1995). *The Official PGP User's Guide*. MIT Press.