Winter 12-5-2004

Trust Models in the E-Commerce Environment

Siddhi Pittayachawan

Mohini Singh

Trust Models in the E-Commerce Environment

Siddhi Pittayachawan, Mohini Singh

School of Business Information Technology, RMIT University
GPO Box 2476V, Melbourne, Victoria 3001, Australia
siddhi.p@ieee.org, mohini.singh@rmit.edu.au

ABSTRACT

This paper analyses several security systems and aggregates their characteristics supporting trust. These characteristics are then matched with e-business models to try and identify the most suitable security system for each model. This is preliminary work undertaken to establish appropriate trust models in the e-commerce environment. The models discussed in this paper are hypothetical.

Keywords: electronic commerce, public key infrastructure, trust, trust model

1. INTRODUCTION

The Internet is the largest global network supporting e-business models, B2B (business-to-business), B2C (business-to-consumer), C2C (consumer-to-consumer), or G2C (government-to-consumer) e-commerce. E-businesses use the Internet to provide product information, online catalogue, electronic transactions, business exchanges, e-negotiations, e-procurement, and online services (e.g. e-government, e-banking and e-insurance) to customers and business partners. New and evolving technologies can be combined with the Internet to enhanced business services. Business organizations around the world are capitalising on the Internet to expand business to organizations and customers to greater geographic regions. Turban et al. [27] emphasise that the benefits of e-businesses include reduced costs, automated and integrated business processes, quick retrieval and dissemination of information, better information management methods, and efficient transactions. In the B2B e-commerce, e-procurement is an important application enabling organisations to reduce purchasing administrative costs by a substantial amount. In the B2C, e-business consumers have the advantage of a 24 by 7 shopfront, access to e-banking and e-government services. [27]. The SMEs (Small and Medium Enterprises) are also capitalising on the Internet to compete with larger businesses.

Although security technologies available off the shelf, these are not always sufficient to prevent the Internet from various kinds of attacks (virus, information access, worms, etc.), an important barrier to e-commerce has been a lack of trust by the Internet users to complete a transaction. Trust has been found to be a crucial factor for e-commerce success [20] due to uncertainty and risk in its nature. As e-commerce environment becomes more uncertain because Internet users are separate from each other by space (e.g. distance between countries) and time (e.g. delayed response on the Internet), the need for trust is very critical [10, 20].

This paper introduces and discusses trust models suitable for different e-business models (e.g. B2C, B2B, B2E, and G2G). These models were developed by analysing the trust mechanisms from several existing trust models, including ITU-T Recommendation X.509 [1], PEM (Privacy Enhanced Mail) [13], PGP (Pretty Good Privacy) [2], PEMToolKit [3], ICE-TEL (Interworking public key Certification infrastructure for Eurpoe) [6], SDSI (Simple Distributed Security Infrastructure) [23], SPKI (Simple Public Key Infrastructure) [8], NPKI (Nested certificate based PKI) [17], and Solar Trust Model [7]. Note that SDSI and SPKI has been merged and become one trust model as the version 2 of SDSI/SPKI recommendations were published in 1997, due to the similarity of these two models. These eight trust models are PKI (Public Key Infrastructure) -based models from either international security standards for IT (Information Technology), purposed models in published paper, or existing models that have been successfully deployed in several business applications.

2. TRUST

Technology trust has been studied for at least half a century. These studies have included meanings [19], characteristics [20], calculation of trustworthiness [18], and the relationships between trust and other factors, such as risk, uncertainty, and confidence [14, 16, 24, 26, 28]. The impact of trust on the human society, business and commercial partners, organisations, and teamwork has also been investigated. Regrettably, to date there is no satisfactory explanation of the nature of trust or its relationship to these entities [24]. As a result, the meanings and characteristics of trust in many technical applications are still imprecise. McKnight and Chervany [20] identified sixteen distinctive categories of trust characteristic definitions (competent, expert, dynamic, predicable, good and moral, good will, benevolent and caring, responsive, honest, credible, reliable, dependable, open, careful and safe, shared understanding, and personally attractive) grouped into five major categories of competence, predicability, benevolence, integrity, and other. Their findings demonstrated that trust is a

relationship that can be seen and used from several perspectives. In this paper, trust refers to one's belief of others in terms of competence, predicability, benevolence, or integrity in the e-commerce environment.

3. TRUST IN E-COMMERCE

The reason why trust has become a very important issue in e-commerce is that the environment and digital processes (e.g. electronic transactions) of e-commerce contain very high risk factors, such as impersonation, fraud, security, privacy, dishonest people, page-jacking, and parallel webs [5, 14, 16, 20, 25, 26]. Hoffman, Novak, and Peralta are of the opinion that almost 95 percent of online users decline to provide personal information on web sites due to a lack of trust [12]. They also suggest that 69 percent of online users did not provide information on web sites because the sites did not provide any information on how the data would be used. Ponemon Institute (http://www.ponemon.org) and TRUSTe (http://www.truste.com) reported that 76 percent of Internet users are concerned about "identity theft" if their personal information were leaked to unauthorised individuals or organisations [11]. Grazioli and Jarvenpaa emphasise that there are approximately 25 million pages, or 2 percent of the total number of pages on the Internet supporting fraud, called "page-jacking" [10].

Trust is important wherever risk, uncertainty, or interdependence exists [20]. Without trust, e-commerce will not be a success [26]. It is one of the most desired qualities in any close relationship. It is indispensable in social relationships, which may lead to significant benefits especially in business relationships [14]. Trust reduces complexity in human society [16]. Similarly, it is a bridge for both a seller and a buyer to cross over uncertainty in the e-commerce environment. Trust problems affect family relationships, business transactions, and client/professional interactions [28]. A buyer wants to buy a quality product with a reasonable price while a seller wants to sell a product and to be well known in the marketplace. In fact, a buyer could be a fraudster or a seller could sell a non-qualified product - or nothing at all in the e-commerce environment.

Before e-commerce had been established, there was only one type of commerce called "brick-and-mortar commerce." In the marketplace, products could be seen, touched, and tested at the point of sale. Tan and Thoen [26] suggest that it is difficult to increase the trust of online users in e-commerce as compared to brick-and-mortar commerce because buyers and sellers cannot see each other and someone could impersonate somebody else, either known or non existent. This makes trust in the online environment very vulnerable. E-commerce is known for receiving payment and not sending the product to the buyer. This occurred with eBay many times. Auction fraud had increased from 106 cases in 1997 to 25,000 cases in 2001 [22].

Another type of risk perceived by the online shopper is losing control over the situation and/or not being familiar with this kind of technology. "Social uncertainty" exists when the seller has an incentive to act in a way that imposes cost or harm on the buyer, and the buyer does not have enough information to predict the behaviour of the seller [10].

4. EVOLUTION OF TRUST MODELS

In 1976, Diffie and Hellman [8] introduced the PKCS (Public Key Cryptosystem), which is a cryptography method, a central authority or public file to support e-mail security. This scheme reduced the risk of key management, which is a method of managing a key pair that consists of a public key and a private key. However, with this method, an impersonation was still possible because no one could ensure that the public key that online users obtained from the trusted public directory really belonged to the claimed entity.

In 1978, Kohnfelder invented the idea of a digital certificate [15]. It was a mechanism designed to link the public key, which is a tool to encrypt a plain message and can be opened by the owner of that key, to a given identity, and signed by a trusted entity such as TTP (Trusted Third Party). Depending on the method of encryption used, the digital certificate could be almost unforgeable, or take a long time to be deciphered. This method solved the impersonation issue previously mentioned and improved the performance of key management for the TTP [8].

In 1988, the CCITT (Commité Consultatif Internationale de Telegraphie et Telephonie), which is now known as the ITU (International Telecommunication Union), published CCITT Recommendation X.509. Part of X.509 was to define and standardise a global, distributed database of named entities, such as people, computers, printers, etc. It also could be described as an online telephone book. However, the plan was not a success because the idea of using a single global name in the world that had countless number of entities was unlikely to be true [8].

In 1989, PEM (Privacy Enhanced Mail) attempted to implement the X.509 standard by the IETF (Internet Engineering Task Force). However, it was delayed due to the long time spent on deploying its infrastructure, including IPRA (Internet Policy Registration Authority), PCA (Policy Certificate Authority), and CA (Certificate Authority) [6].

In 1991, Zimmermann [2] introduced new secure-communication software known as PGP (Pretty Good Privacy). The structure of PGP was different from X.509 and PEM. Unlike PEM that had to wait for the

establishment of a single global root and a hierarchy of CAs, PGP allowed a digital certificate to be signed by anyone, and could contain multiple digital signatures. This approach enabled several virtual communities to be quickly established and grown due to the "Six Degrees of Separation" theory, which describes how someone can connect to anyone in the world through the chain of intermediaries containing not more than six people [4], and was well known as the "web of trust" model.

In 1992, the NSF (National Science Foundation) enabled commercial companies to conduct business transactions securely over the Internet. With the establishment of this large global network, many companies lodged business online. However, the Internet was not suited for a commercial environment and was not developed with security in mind [14]. It was meant for sharing information in plain text format.

5. TRUST MODEL ISSUES

A trust model should be able to support trust relationships that are required by users and online businesses, and to provide control mechanisms that allow them to establish and enhance trust. Therefore, it is important to understand the characteristics and needs of target community and users, and to create and embed these characteristics into a trust model [6]. The framework of a trust model is an important factor to determine how the model will be used and whether it is suitable for the target virtual community. The framework of a trust model in this paper refers to trust mechanisms to manage trust relationships between buyers, sellers, suppliers and other relevant parties. If the target community is a small group of casual end-users but a trust model uses a very strict security policy, then model deployment, user registration, and cross certification will be very difficult and slow to manage. This happened with PEM that contains very strict security policy and requires deploying several central authorities before any user is able to communicate with each other securely. On the other hand, if the target community is made up of a large number of end-users and CAs but the trust model lacks a standard security policy, then that virtual community will not be able to function successfully. PGP can be associated with this characteristic because it contains no standard security policy, and therefore, it is not easily scalable when hundreds of thousands of users are involved [6].

Although a trust model is not only a security system [14, 16], in this paper, it is based on the analysis of PKI-based security systems. Security system in e-commerce is different from security in traditional networks. There are four major security issues in e-commerce [25]:

- Authentication – communicating parties must be certain of each other's identity and/or credentials;
- Confidentiality – data must not be visible to eavesdroppers;
- Integrity – communicating parties must know when data has been tampered with; and
- Non-repudiation – it must be possible to prove that a transaction has taken place.

However, Skevington [25] argued that this approach is inadequate in the open and distributed environment of the Internet. Trust must be embedded into infrastructure, data, and user identity.

6. RESEARCH METHODOLOGY

The research discussed in this paper was inspired by a lack research on trust mechanisms illustrating how trust models perform or apply to e-commerce business models. It is based on a document analysis methodology. The findings in this paper were compiled using a categorical aggregation analytic strategy. Categorical aggregation is the process of piecing together bits of information gathered regarding an issue and organising it into an orderly research interpretation [29]. Each of these categories is further broken down into nominal attributes (non-numeric and unordered elements) using both homogeneous and heterogeneous decomposition methods. Goldstein and Roth [9] stated that there are two types of decomposition. Homogeneous decomposition is to use the same attribute to repeatedly partition a group by choosing more narrow ranges of the attribute's values. Heterogeneous decomposition, on the other hand, is to use different attribute to decompose sets for successive partitions.

7. FINDINGS

An analysis of eight trust models chosen for this research revealed that some of the findings are common to all while some are quite different. Trust models examined in the research are all PKI-based. The research found that there are 25 trust mechanisms in the chosen trust models. Although the value or importance of trust mechanisms were not identified, these trust mechanisms were ranked based on the opinions of [2, 3, 6-8, 17, 21, 23] who previously stated in their works, the commonality of trust models, and the effect of these mechanisms on communities when attributes were changed. In this paper, an attribute is a sub-category of a trust mechanism. Table 1, which is presented at the conference, shows trust mechanisms and their attributes in the trust models commonly used. The horizontal top column shows the name of each trust model. The vertical left-most column lists trust mechanisms. Each trust model uses different attributes to create. Some trust models support more attributes than others. This illustrates that they are more flexible than other models. However, it does not mean that they can support more kinds of e-commerce models. An appropriate combination of trust mechanisms is crucial in order to develop a trust model suitable for each kind of e-commerce models.

8. TRUST MODELS

In order to determine the most appropriate trust model for an e-business model, trust mechanisms are matched with the interaction between participants. The behaviour of a trust model may affect how users interact with each other, what kind of information (e.g. user's identity, security policy) is available, how information can be validated or delivered, what kind of environment is used (e.g. user-friendly interface, control mechanisms), and for which e-commerce model is suitable. Trust mechanisms are used to assist in the development of the framework of a trust model for each e-commerce model.

In this section, seven conceptual trust models are discussed. These models were developed from 25 trust mechanisms presented in Table 1. The combinations of attributes of trust mechanisms are based on the application and the type of network in which the hypothetical e-commerce model operates. The models are discussed from the smallest community containing the simplest trust relationships (e.g. relationships between friends, family, relatives, and team-mates), to the largest community containing very complex trust and several kinds of trust relationships (e.g. relationships between business partners, companies, government, organisations). The model starts from the simplest trust relationships or close relationships.

8.1 Close-Relationship Trust Model (B2E, B2C)

The simplest human society starts from close relationships that are established directly between relevant parties (PGP Corporation 2003). It contains the highest level of trust because members in this community know each other very well. It also needs the least secure environment, which makes this trust model very simple, compared to other sample trust models in this section. Figure 1, which is presented at the conference, illustrates a small group of end-users that have agreed to establish an internal network with a convenient communication method based on an adequate security system.

This type of trust model could be used for private trust relationships such as friends, members in the family, relatives, colleagues, or a group of people that know each other well, and this makes the community small. Thus, there is no need for any formal proof signed by some trustworthy entities. It may not need a strict security policy unless there is some very sensitive information that needs to be shared among a few exclusive members in the same community. In the e-commerce context, it may apply to a small B2C enterprise that contains single security domain or B2E (Business-to-Employee) e-commerce, an Ethernet, or the requirement of establishing a secure communication channel (e.g. e-mail).

Members in this small community are assumed to be familiar with each other and do not need a central authority because it is a close domain. Therefore, the structure is anarchy, growth is organic, trust management is decentralised, and trust relationships are managed by a trusted entity. There is no standard security policy and trust transitivity in this model because members do not need to contact people in other communities. From Table 1, it can be said that PGP is most suitable for this e-business model.

8.2 Casual Trust Model (B2C, B2B)

A casual trust model in this paper refers to the illustration in Figure 2 (presented at the conference) when:

- Users need to contact other users, who are members in different security domains;
- Users need to create a central authority for enabling a standard security policy for user authorisation system; and/or
- Users need to strengthen the security level throughout their community.

With any of these reasons, a security policy must be standardised and this means that a community needs to establish a central authority. In this paper, a central authority is a person who is responsible for validating the identity of members, signing digital certificates, creating security policy, issuing cross certificates, and maintaining the network. Thus, this trust model is suitable for a medium enterprise that contains a few different security domains. In B2B e-commerce, two companies need to establish security communication channels between several security domains (e.g. sending or sharing sensitive information between two companies. In B2C e-commerce, a customer needs to do business with a company.

Members in this community need to contact people in other communities, presumably in an e-commerce environment containing a few companies and customers. Security policy is needed to properly standardised in order to enable cross certification, which is a task done by a central authority. Therefore, the structure is both hierarchy and anarchy, growth is both scalable and organic, trust management is both centralised and decentralised, trust relationships are established by either a trusted entity or a trusted path. These cover security policy and trust transitivity. From Table 1, it can be said that ICE-TEL is the most suitable for this e-business model.

8.3 Community Trust Model (B2C, B2B, G2C, G2G)

A community trust model is used when:

- Users need to establish proper formal small communities on the Internet;
- Organisations need to set up a trustworthy network for secure communication; or

- Companies want to create their communities in order to deploy an e-commerce environment and applications.

In this model, there would be more than one type of trust relationship because it is an open community, which anyone could join in. This does not limit them to only a close-relationship as it does in the trust models previously discussed. Possible types of trust relationships may include close relationship, acquaintance, friends, family, colleagues, co-workers, customers, business partners and other distant relationships (e.g. third parties). An appropriate set of security policies is needed in order to prevent hackers and malicious attacks. This trust model is suitable for an open community where there are several kinds of companies and organisations in the same environment, e.g. B2B or G2G exchanges of goods between large and small organizations or suppliers and distributors, or B2C or G2C e-commerce where customers need to filter unrelated companies and measure the trustworthiness of related companies.

A number of e-commerce organisations are large and contain different sizes of companies and businesses. Members in this community need a more sophisticated trust model for trust management. A suitable structure for this will be both hierarchy and anarchy, scalable and organic growth with trust management both centralised and decentralised. From Table 1, it can be said that ICE-TEL is suitable for this e-business model.

8.4 Community with Casual Trust Model (B2C, B2B, G2C, G2G)

This model has the same characteristics as the community trust model with an extra environment for users to create their own private communities. It is actually a casual community inside the community trust model. This means that this trust model contains a community trust model as a primary model, and a casual trust model, as a secondary trust model. Therefore, users can create casual communities, and save time and bandwidth requirements in the process of verifying identities. This model is suitable for a larger scale community compared to the previous models. For example, a virtual community where there are several companies, governments, and users in the same environment; it will incorporate central system administration domain, and share sensitive information between several member companies in the same department that contains members from different companies or organisations. Another example is that a large company that contains several large divisions or sub-companies, and wants to create a new special division that contains a few selected members from different divisions.

For this, bottom-up virtual society establishment, which is a unique feature of PEMToolKit, is chosen. From Table 1, it can be said that ICE-TEL is the most suitable for this e-business models.

8.5 Organisational Trust Model (G2G)

An organisational model is to be used for a large organisation having a solid structure that is unlikely to be changed, or a community that contains very sensitive information and needs very secure communication channels. One of the most suitable business models is G2G (Government-to-Government). Hence, it is crucial to not only to increase trust but also reduce risk in a community. Members in this community need a very secure and solid model. Trust relationships established by users are not allowed in order to minimise risk. In fact, this community seeks more security rather than trust. From Table 1, it can be said that X.509 is the most suitable for this e-business model.

8.6 Popularity-based Trust Model (C2C, P2P)

This model is based on the popularity of each user. It may be used with a measurement of trustworthiness of users in some closed communities, such as an online auction, bookshop, or e-commerce company search engine. For example, it would be better if an online auction could provide trustworthy information about buyers or sellers before transactions have been processed. The trustworthiness value would be determined by how many digital signatures have been signed on the digital certificate of the target and who signs those digital signatures.

In this model, if a member registers online, then a central authority would not sign on a digital certificate because it is too difficult to trust and verify all information provided digitally from a faceless member. However, if a member registers at a physical office, then a central authority would verify proof of identity (e.g. driving license, social security number, passport or other personal id cards). A central authority would then help one to generate a key pair with a digital certificate signed by a central authority. This process is long but it counterbalances the problem of new members having no trustworthiness information. The local business registrar should be responsible for this task, as all companies must be registered with the government organisations before commencing any business. However, a central authority could revoke the digital signature for any member if there is any suspicion. Therefore, trust relationships in this trust model would be changed dynamically by comparison with other trust models. This trust model is suitable for a large community that contains members with the same level of authorisation and needs the value of trustworthiness or background information of users in order to decide which one is trustworthy enough to do the business. One of the suitable business models using popularity-based trust model is C2C (Consumer-to-Consumer), P2P (Peer-to-Peer) or auction-based e-commerce environment.

Figure 7, which is presented at the conference, illustrates how this model is superior to other models previously discussed in this section. Members in this closed community need a dynamic and flexible trust relationship. Therefore, structure is anarchy, growth is organic, and trust management is decentralised. From Table 1, it can be said that PGP is the most suitable for this e-business model.

8.7 Integrated Trust Model

This trust model is the combination of casual, community, organisational, and popularity-based trust models. It is a trust model, which could support different kinds of trust relationships in the same or across communities. This trust model is suitable for a very large and complex community that contains many relationships. In addition, both central authorities and end-users are included. End-users are also able to create their own communities in order to create either open or closed communities. In fact, this model will be used when all models above have been already deployed and users need to standardise or unify their communities in order to establish secure communication channels conveniently. Suitable e-business models that can use this model are B2C, B2B, G2C, and G2G when calculation of trustworthiness is important.

An integrated trust model firstly uses a hierarchical structure as a backbone in order to properly define and distribute a set of security policies for different security domains. If a community is very large and contains different types of members, then an IPRA (Internet Policy Registration Authority) and PCAs (Policy Certificate Authorities) may be needed. The part involving an IPRA to a CA is an organisational trust model, and the part involving a CA to an end-user is a community trust model. From Table 1, it can be said that ICE-TEL is most suitable for this e-business model.

9. CONCLUSION

In this paper, a first attempt has been made to match appropriate trust models to e-commerce models for managing trust. Further work will be done to prove the discussion in this paper.

REFERENCES

[1] ITU-T Recommendation X.509, "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks," March, 2000

[2] "An Introduction to Cryptography," PGP Corporation, June 2004 http://www.pgp.com [Accessed 28 September 2004]

[3] Bahreman, A., "PEMToolKit: Building a Top-Down Certification Hierarchy for PEM from the Bottom Up," presented at Proceedings of the 1995 Symposium on Network and Distributed System Security (SNDSS), San Diego, California, USA, 1995.

[4] Blass, T., "Stanley Milgram," 29 September 2003 http://www.stanleymilgram.com [Accessed 9 January 2004]

[5] Castelfranchi, C. and Y.-H. Tan, "The Role of Trust and Deception in Virtual Societies," presented at Proceedings of the 34th Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, USA, 2001.

[6] Chadwick, D. W., A. J. Young, and N. K. Cicovic, "Merging and Extending the PGP and PEM Trust Models - The ICE-TEL Trust Model," in *IEEE Network*, vol. 11, 1997, pp. 16-24.

[7] Clifford, M., C. Lavine, and M. Bishop, "The Solar Trust Model: Authentication without Limitation," presented at Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC), Scottsdale, Arizona, USA, 1998.

[8] Ellison, C. M., B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, IETF RFC 2693, "SPKI Certificate Theory," September, 1999

[9] Goldstein, J. and S. F. Roth, "Using Aggregation and Dynamic Queries for Exploring Large Data Sets," presented at Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Celebrating Interdependence, Boston, Massachusetts, USA, 1994.

[10] Grazioli, S. and S. L. Jarvenpaa, "Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers," in *IEEE Transactions on System, Man, and Cybernetics - Part A: Systems and Humans*, vol. 30: IEEE, 2000, pp. 395-410.

[11] Greenspan, R., "Consumers Trust eBay," Ecommerce-Guide.com, 16 June 2004 http://www.ecommerce-guide.com [Accessed 14 July 2004]

[12] Hoffman, D. L., T. P. Novak, and M. Peralta, "Building Consumer Trust Online," in *Communications of the ACM*, vol. 43, 1999, pp. 80-85.

[13] Kent, S., IETF RFC 1422, "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management," February, 1993

[14] Kini, A. and J. Choobineh, "Trust in Electronic Commerce: Definition and Theoretical Considerations," presented at Proceedings of the 31st Hawaii International Conference on System Sciences (HICSS), Kohala Coast, Hawaii, USA, 1998.

[15] Kohnfelder, L. M., "Towards a Practical Public-Key Cryptosystem," in *Department of Science*: Massachusetts Institute of Technology, 1978, pp. 51.

[16] Konrad, K., G. Fuchs, and J. Barthel, "Trust and Electronic Commerce - More Than a Technical Problem," presented at Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems (SRDS), Lausanne, Switzerland, 1999.

[17] Levi, A. and M. U. Caglayan, "An Efficient, Dynamic and Trust Preserving Public Key Infrastructure," presented at Proceedings of the 2000

IEEE Symposium on Security and Privacy (S&P), Berkeley, California, USA, 2000.
[18] Marsh, S. P., "Formalising Trust as a Computational Concept," in *Department of Computing Science and Mathematics*: University of Stirling, 1994, pp. 163.
[19] McKnight, D. H. and N. L. Chervany, "The Meanings of Trust," MIS Research Center, University of Minnesota, 1996 [Accessed 29 September 2004]
[20] McKnight, D. H. and N. L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," presented at Proceedings of the 34th Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, USA, 2001.
[21] Perlman, R., "An Overview of PKI Trust Models," in *IEEE Network*, vol. 13, 1999, pp. 38-43.
[22] Reuters, "Read this before buying on eBay," Lycos, Inc., 9 January 2003 http://www.wired.com [Accessed 28 January 2003]
[23] Rivest, R. L. and B. Lampson, "SDSI - A Simple Distributed Security Infrastructure," 30 April 1996 http://www.syntelos.com/spki [Accessed 28 September 2004]
[24] Robles, S., S. Poslad, J. Borrell, and J. Bigham, "Adding Security and Privacy to Agents Acting in a Marketplace: A Trust Model," presented at Proceedings of the 35th International Carnahan Conference on Security Technology (ICCST), London, England, 2001.
[25] Skevington, P. J., "From Security to Trust - Creating Confidence to Trade Electronically," presented at Proceedings of the IEE Colloquium on eCommerce - Trading But Not As We Know It, London, England, 1998.
[26] Tan, Y.-H. and W. Thoen, "Formal Aspects of a Generic Model of Trust for Electronic Commerce," presented at Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, USA, 2000.
[27] Turban, E., D. King, J. K. Lee, and D. Viehland, *Electronic Commerce 2004: A Managerial Perspective*, 3rd Edition ed: Prentice Hall, 2004.
[28] Webb, W. M. and P. Worchel, "Trust and Distrust," in *The Social Psychology of Intergroup Relations*, W. G. Austin and S. Worchel, Eds. Monterey, California, USA: Brooks/Cole Publisher, 1979, pp. 213-228.
[29] Wilson, B. B. and D. L. Stewart, "Employers' Perceptions of Welfare Reform: Implications for Cooperative Extension Personnel," *Journal of Extension*, vol. 38, 2000.