

A Trusted Approach to E-Commerce

Giannakis Antoniou¹, Lynn Batten², and Udaya Parampalli¹

¹ The University of Melbourne
Department of Computer Science and Software Engineering
{gant, udaya}@csse.unimelb.edu.au

² Deakin University
School of Information Technology
lmbatten@deakin.edu.au

Abstract. It has been well documented that lack of trust between commercial entities and purchasers can restrict the potential of e-commerce. This may be because the purchaser is required to provide sensitive information to the commercial entity or because the purchaser may be suspicious that after payment has been processed, the goods purchased will not arrive. The challenge for the researcher is to determine the e-commerce model which maximizes the trust relationship. In this paper, we introduce a measure of the trust based on the information distributed to the parties in the transaction and isolate the instances which maximize trust for the purchaser. This leads us to propose four new models for e-commerce which would improve consumer trust and therefore likely lead to an increase in on-line commerce. We demonstrate that no new technologies are needed in order to implement these new models.

Keywords: Trust, E-Commerce, Privacy.

1 Introduction and Background

The convenience to consumers of remote twenty-four hour access to products online has driven e-commerce popularity [5, 15, 18]. However, many writers have argued that this same 'remoteness' has restricted the full potential of e-commerce because the purchaser may be asked to provide sensitive information to an unknown entity over the Internet and does not know how their information will be treated [7]. These studies underline the important role of trust in e-commerce [12, 13] and argue that some purchasers do not trust sellers because of a number of risks derived from the very nature of e-commerce.

A purchaser who wants to buy a product online searches for a seller of the product and is restricted to making a purchase only from a seller who can provide the needed product. Given a choice of sellers, the purchaser will normally choose one with whom the purchaser has completed a successful transaction in the past [4]. If this is not an option, the purchaser must make a decision based on other factors. In making this decision, the purchaser may consider such issues as how much of his personal information (full name, age, sex, address and email) will be distributed to other entities and whether or not his payment details (credit card information, amount of purchase) will be misused. He may also wonder how and where his information will be stored – will it be in a secured environment or vulnerable to attackers, will it be made available to

spammers. Moreover, the purchaser may worry about receiving the product once it is paid for. The reputation and credit-worthiness of the company may be a factor, or the range of products and services offered for potential future transactions.

Several models [3, 19] have been formulated to assist in attaining a sufficient trust level on the part of the purchaser. For example, several payment systems have been proposed which allow the purchaser to pay anonymously [8, 16]. It has also been argued that the attractiveness of an online shop is a factor in increasing trust. This has led to such inventions as virtual reality e-commerce [11]. While the key focus in all approaches has been on the relationship between the purchaser and seller, we point out that the financial organization and the deliverer of the goods need to be considered.

In [10] the definition of trust is “a trustor’s expectations about the motives and behaviours of a trustee”. We adopt this definition in the e-commerce setting where a purchaser has a number of expectations of several parties. We argue that the financial organization (the bank supplying the credit card) involved in an online transaction is chosen well in advance by the purchaser, has a well established relationship with him and so is expected to act ‘as usual’ in completing the financial transaction component of a purchase. The purchaser has a good understanding of the motives and behaviours of the financial company. We also argue that the deliverer of the goods purchased may be chosen by the purchaser and can therefore be an organization with which the purchaser has a long-standing or trusted relationship. In many cases, the deliverer would be the national postal service which has delivered goods to the purchaser for many years.

In this paper, we consider all three of these players (*seller*, *financial organization* and *deliverer*) from the point of view of the purchaser and examine the aspects of trust associated with each. We use only that information necessarily disclosed by the purchaser, which is essential to the transaction. We use this analysis to develop a model which optimizes the trust, from the perspective of a purchaser, in an e-commerce transaction. We also describe the technologies used in existing models and demonstrate that these same technologies are sufficient for the proposed models.

In section 2, we discuss the various kinds of information a purchaser is required to disclose in an e-commerce transaction. In section 3, we present an abstracted model for the e-commerce transaction situation. In section 4, we introduce a method of measuring the privacy concerns of a purchaser. Section 5 analyzes the traditional e-commerce models and compares these with the proposed models from the point of view of the theory of section 4. In section 6, we propose an implementation of the new models and demonstrate that no additional technologies are required. Section 7 concludes the paper.

2 Purchaser Information

The information that a purchaser is likely to reveal to a party in an e-commerce transaction, but wants to protect from others, can be divided into the following categories:

Order Information: Information related to the characteristics of the product which can identify the product.

Delivery Information: Information which identifies the source and the destination of a delivered product (address or box number).

Payment Information: Information such as credit card number or social security number.

Personal Information: This includes name, age, email address and sex.

We assume that this information is sufficient to conclude a transaction and that the purchaser wishes all of the information to be kept confidential or private.

We argue that the level of trust expected in an e-commerce relationship is directly related to the purchaser's expectation of how the above information will be used or misused. Therefore, the abstract models we build in the following section are based on the transfer of the above information from the purchaser to the parties mentioned in the previous section.

Usually, a purchaser reveals personal information when registering with a seller. The seller also receives the order information and often, also the financial and delivery instructions [21]. Separately, these pieces of information may not be useful to a malicious entity, but combined, they reveal the identity of the purchaser along with credit card information and possibly his desires, habits, financial and health condition. This information may be used for the purposes of impersonation, theft, bribery or blackmail.

Our goal is therefore to introduce a measure of the value of combinations of the purchaser's information and a set of transactions between the parties which minimizes this value. We do this in the next section.

3 Abstract E-Commerce Models

In the models described in this paper, we assume that a transaction is electronic but that the product purchased requires physical delivery by a deliverer. We treat the deliverer as an entity distinct from the seller as often an e-shop will use the national postal service for delivery of goods. We also assume that the purchaser uses an e-payment system to pay and that payment is made by credit/debit card issued by a financial company. In any such e-commerce transaction the minimum information which a purchaser needs to reveal is:

- 1- Order Information
- 2- Delivery Information
- 3- Payment Information

Here we argue that the *Personal Information* of the purchaser identified in section 2 is not needed in order to successfully complete an online transaction. The three pieces of information listed above are sufficient.

Before turning to the abstract model, we point out also that some realizations of electronic consumer to business transactions involve proxies for the seller or deliverer (but usually not the financial organization). Our initial aim is to identify all possible models under the above assumptions based on the flow of information. We assume

additionally that the seller knows at least the Order Information (1), the deliverer knows at least the Delivery Information (2) and the financial company knows at least the Payment Information (3). For every entity there are thus precisely 4 combinations yielding a total of 64 combinations of models as illustrated in Table 1.

For example, a seller may know:

- Order information - 1
- Order and Delivery information - 1, 2
- Order and Payment information - 1, 3
- Order, Delivery and Payment information - 1, 2, 3

Table 1. The 64 abstract e-commerce models

Entities	Models	Mi
Seller		1 ? ?
Deliverer		2 ? ?
Financial Organization		3 ? ?

In narrowing the set of models further, we again consider the perspective of the purchaser who, if paying by credit or debit card, already has an established relationship with a financial organization. We can assume that the relationship between the purchaser and this financial organization is a trusted one relative to payment information. Additionally, in considering the deliverer, we assume that the seller will use a well established organization such as a national postal service or that the purchaser may choose the deliverer. In either case, we assume that the purchaser is able to rely on a trusted delivery service.

On the other hand, in selecting the seller, the purchaser is restricted to choosing a seller from the set of sellers who own the object which the purchaser wishes to purchase. It is the object for purchase which is the key factor; the choice of seller is based on this object. Hence, the purchaser does not have unrestricted choice of seller. Thus, the seller may be a company not known to the purchaser and whose reputation is unavailable. The seller may in fact be located in a country where rules concerning the distribution of the private information about clients do not exist. For example, the lack of privacy recognition in India [14] may discourage potential purchasers worldwide to buy from that country. For these reasons, we argue that the relationship between the seller and purchaser is in most cases the least trust-worthy. It follows that the best possible model with regard to preserving the privacy of the purchaser is one in which the seller only has access to the order information.

We would also argue that a financial institution would not want the encumbrance of information about purchases other than the ones necessary to execute the financial component of the transaction. Nor do they need extraneous information. Hence, we will assume that the financial organization only has access to the payment information of the purchase.

We have thus established two hypotheses:

- 1) The seller should know only the order information
- 2) The financial organization should know only the payment information.

Based on the above hypotheses this reduces us to four e-commerce models, eliminating 60 models.

Table 2. Four e-commerce models under hypotheses 1 and 2

Entities	Models	M1	M2	M3	M4
Seller		1	1	1	1
Deliverer		2	1,2	2,3	1,2,3
Financial Organization		3	3	3	3

We refer to these four models as the ‘*trust-enhanced*’ models. It remains to examine the practicality of implementing these four cases.

The M1 model is most appropriate for an e-commerce environment in which a purchaser does not trust any entity. For instance, this model may be useful in communities where corruption is very high. Nevertheless, the necessary communications between the seller and financial organization, to authorize the transaction, and between the seller and deliverer, to pass on the product, may be untrustworthy from the purchaser’s point of view.

Each of the models M2, M3 and M4 is appropriate where a purchaser trusts the deliverer to some extent. If the payment information is held to be more ‘valuable’ by the purchaser than the order information (or vice-versa), this will impact on which of these models to choose. The M3 model is appropriate where a purchaser buys goods which reveal sensitive information about the purchaser, such as sexual preferences or medical problems. The M4 model is appropriate where, for instance, the purchaser’s community requires a level of transparency for security reasons in order to prevent the purchaser from buying illegal goods from outside of the community. We therefore introduce measurements by which we can better analyse these four situations. This measurement system can be applied to all sixty-four models in Table 1.

4 Measuring the Privacy Concern of Purchasers

As we have indicated in the Introduction, the level of privacy concern of purchasers for an e-commerce model is a major factor in the success of that model. Therefore, it is important to have a mechanism measuring the level of privacy retained by each of our models. From the point of view of the purchaser, a violation of privacy may occur where there is little trust between the purchaser and another entity in the transaction (in this case, the seller, deliverer or financial organization). In addition, the more sensitive the information disclosed, the greater the impact on privacy loss. We therefore use these two significant items as the basis of our measurement of an expected

privacy violation [1], [17]. We refer to the level of mistrust between the purchaser and the other entities as *Level of Mistrust* [17], indicated by T, and use W to indicate the level or *Weight of Sensitivity* [1] of information disclosed. T can be indexed by the three entities and W by the three types of information, as indicated in Table 3. The actual values of these parameters can be taken from any set of non-negative ordered numbers. Obviously, different scales may be used for each of T and W.

Table 3. The notation used for measuring the privacy concern of a purchaser

Notation	
T	Level of Mistrust
W	Weight of Sensitivity
x	(seller, deliverer or financial company)
i	(order, delivery or payment information)

We now define **P to be the expected privacy violation** associated with a model from the perspective of the purchaser.

Let $P_x = T_x \sum^x (W_i)$ be the level of mistrust a purchaser has in an entity x multiplied by the sum of only those pieces of information W_i provided to entity x in a particular model as in Table 1. This measures the expected privacy violation between the purchaser and entity x. The total expected privacy violation in a transaction represented by this model is then the sum over all P_x or $P = \sum P_x$.

A low value for **P** indicates a low level of violation of privacy, whereas a high level indicates a high privacy violation. If a value of 0 is assigned to any T_x , then the value of the sum of the weights is eliminated whether this is high or low. In order to maintain the impact of the sensitivity, we suggest taking 1 as the smallest value for T_x .

In computing the expected privacy violation for the four models of Table 2, we note that value for M1 will always be lower than the values for M2, M3 and M4, and that the value for M4 will always be the largest. However, the value for M2 may be smaller or larger than the value for M3.

We present a case example demonstrating how the expected privacy violation for the four models of Table 2 can be computed. The scale for weight of sensitivity and level of mistrust has been chosen by the purchaser to be the discrete set {1, 2, 3, 4, 5} where the values 1 and 5 correspond to the minimum and maximum levels respectively of mistrust or sensitivity. In order to demonstrate the affects of the interactions between the purchaser and the other entities, we keep the sensitivity weights W_i constant.

Case Study: Alice has just received a credit card from her new bank. It is a large, well-recognized bank with a good reputation, so despite the fact that she has not used it before, she is fairly confident that she will have no problems. She wishes to purchase a new television from an online company which she does not know. It offers the brand, size, features and colour she wants at the best price. The seller will ship it using Australia Post. Although she has never before had a large, breakable object shipped to her by Australia post, she has successfully received many items through them in the past.

As she does not want possible burglars to know about her purchase, she assigns a common sensitivity of 2 to the weights of each of the order, delivery and payment information. Because she has no experience with the seller and does not know anything about it, she attaches a (highest) weight of 5 to the level of mistrust; to each of the deliverer and financial organization, she allocates a weight of 2.

The four models of Table 2 can then be analysed from her point of view in the expected privacy violation, \mathbf{P} , and she can see which of these models is best.

$$\begin{array}{ll} T_{\text{seller}}=5 & W_{\text{order}}=2 \\ T_{\text{deliverer}}=2 & W_{\text{delivery}}=2 \\ T_{\text{financial}}=2 & W_{\text{payment}}=2 \end{array}$$

Models	M1	M2	M3	M4
Score	18	22	22	26

Clearly, the most attractive model for Alice is M1 followed equally by M2 and M3. In weighing comparative differences in models with respect to the value of \mathbf{P} , a purchaser faced with a choice should consider the variation in values between M1 and M4. If this variation is large, M4 should be avoided. If it is small, then any one of the four models may be acceptable.

5 Existing E-Commerce Models

In this Section we describe and analyse two e-commerce models currently in use on the Internet. These models are not trust-enhanced as, in each, information other than order information is revealed to the seller. From the perspective of the purchaser, the two models are indistinguishable. However, the flow of the purchaser's private information differs in the models. The first model we refer to as the 'no proxy model' in which a purchaser deals only with entities he can identify. The second we call the 'proxy model', in which additional entities play a role not known to the purchaser. We may refer to both simultaneously as the 'traditional e-commerce model'.

5.1 The No Proxy E-Commerce Model

The participating entities in what we refer to as the no proxy e-commerce model are a purchaser, a seller, a financial organization and a deliverer. The process of the e-commerce model (Figure 1) is described below:

A purchaser requests information about a product (step 1). The seller replies with the related information, including the price of that product (step 2). If the purchaser is satisfied with the price, he requests delivery options and their costs (step 3). After the delivery options and their costs are provided (step 4) by the seller, the purchaser decides whether to buy the product or not. If the decision is yes, he sends the payment details (e.g. credit card information), the selected delivery option and his personal information, such as the telephone number, e-mail address, and the full name of the purchaser (step 5). Hence the seller obtains all order, delivery, financial and personal

information from the purchaser and stores it in a database in order to use it for marketing purposes [6]. After the seller ensures that the payment information is valid (step 6) and obtains payment (step 7), it prepares the product for delivery by the deliverer. The seller gives the product to the deliverer, including the full delivery address (step 8). The seller also pays the deliverer based on the selected delivery option of the purchaser. Finally the deliverer delivers the product to the purchaser (step 9). Examples of this e-commerce model are Amazon (www.amazon.com) and Mayer (www.mayer.com).

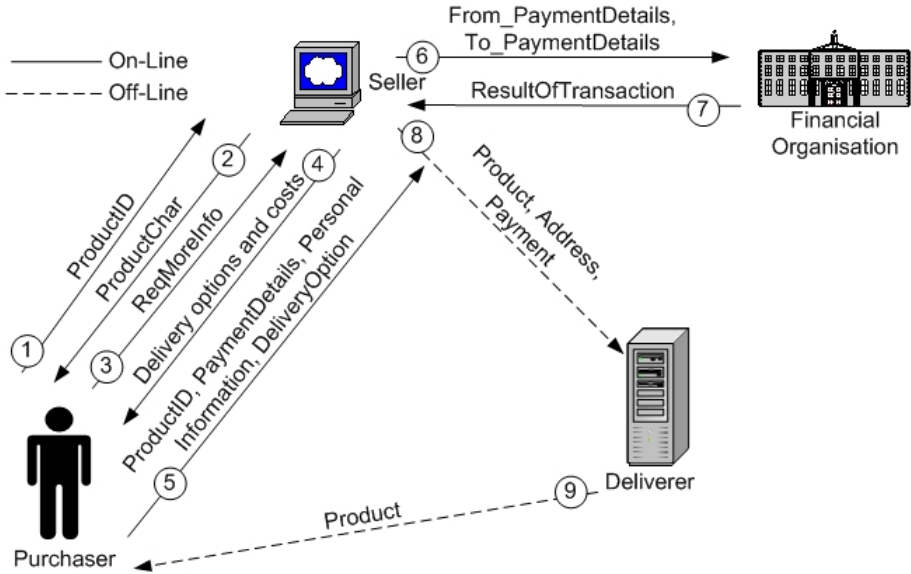


Fig. 1. The no proxy e-commerce model

The no proxy e-commerce model falls into the following model type.

Entities	Model	No Proxy Model
Seller		1,2,3
Deliverer		2
Financial Company		3

In this model, the distribution of the purchaser’s personal information (steps 3 and 5) raises a number of privacy and security issues. The purchaser’s information is stored in a database for a period of time length of which is decided by the seller. A database which contains vast amounts of personal information and credit card details is a target for attackers [9]. An additional factor for consideration is what happens to the data that sellers hold when they close down or are sold to another company. If the head office moves from one country to another, what impact does the changing legal

scene have on the way this data is held and managed? In such a situation, one should expect the mistrust level by the purchaser to be high.

According to [2, 20], sellers can increase their customer base by increasing the appearance of trust; therefore, it is desirable to have a trustworthy system which is responsible for data handling including confidentiality of personal information and accountability of sellers' actions. The traditional e-commerce model demands a high level of trust because of the high level of risk that purchasers and sellers face. Taking into consideration the dissemination of the personal information, the flow of information is as in Table 4 below.

Table 4. Information each entity has about the purchaser in the no proxy model

	Seller	Deliverer	Financial Organisation
Personal Information	√	×	√
Payment Information	√	×	√
Order Information	√	Limited	Limited
Delivery Information	√	√	×

5.2 The Proxy E-Commerce Model

Companies, especially small companies, who want to sell their products on-line, sometimes transfer a portion of the responsibility to a provider of online services which we call a proxy. For example, a small business supplier of honey may wish to sell its products through a large online supermarket. To a purchaser, the seller appears to be a trustworthy online seller, but in fact, the small business receives payment and delivers the product. We refer to a company which sells its products via another organization as 'product-oriented' (POC). Essentially, the transaction steps of the no proxy model are followed but an extra party is involved in some of the steps. The supermarket company (SC) may act as a direct seller of goods obtained from wholesalers, along with goods from a number of POCs. The SC is responsible for the website and the online purchasing. Each POC makes available the information about their products on the SC's web site. A purchaser visits the SC's web site (without seeing identification of the POCs), finds the desired product and pays the SC who then informs the relevant POC and the POC arranges for delivery of the item. The POC has no access to the financial and personal information of the purchaser

As an additional, somewhat different, example, Yahoo! operates as a proxy on behalf of a number of POCs and is responsible for handling the payment system, hosting the web site and the database, informing the POCs of the orders and generally taking on the technical responsibilities such as web development, web hosting, and e-payment. The POCs are responsible for updating the content of the web sites (such as product pricing, available offers etc) and arranging for the delivery of the products. Yahoo! itself does not sell its own products in this system. While in this case, a POC does not have access to the payment information of a purchaser, it has access to the personal, order and delivery information.

Thus, in the proxy model, a purchaser may not know who has access to his sensitive information and so has no way of determining with any accuracy the trust level required in the transaction.

In the tables below we represent the flow of information. The model type is the same as that for the no proxy case, so we do not give the table. The first chart gives the general proxy situation. Note the very small difference between Tables 5 and 6.

Table 5. Illustrates the type of information each entity has in the Yahoo! proxy e-commerce model

	Yahoo!	Small Business	Post Office	Financial Company
Personal Information	√	√	×	√
Payment Information	√	×	×	√
Order Information	√	√	Limited	Limited
Delivery Information	√	√	√	×

Table 6. Illustrates the type of information each entity has in the e-Supermarket model

	Supermarket	Small Business	Post Office	Financial Company
Personal Information	√	×	×	√
Payment Information	√	×	×	√
Order Information	√	√	Limited	Limited
Delivery Information	√	√	√	×

5.3 Comparison of the Trust-Enhanced and Traditional E-Commerce Models

In the case of the no proxy model, it is possible to apply the measurements of section 4 with precision. In the case of the proxy model, we can only determine the best case expected privacy violation figure, as the values assigned to unknown entities are not computable.

Clearly, a good e-commerce model should be transparent to the purchaser, indicating all the parties involved and allowing the purchaser to determine with accuracy the level of privacy violation which may occur.

To compare the trust-enhanced model with the proxy and no proxy models, we recall the case study of section 3. The table below shows these same values for T_i and W_i as were used in the study (Case 1) and gives the values for a possible second case.

Models Cases	Proxy & No Proxy	M1	M2	M3	M4
Case 1: $T_{seller}=5, T_{deliverer}=2, T_{financial}=2, W_i=2$	38	18	22	22	26
Case 2: $T_{seller}=W_{order}=5, T_{deliverer}=T_{financial}=W_{deliverer}=W_{payment}=2$	59	33	43	37	47

Observe that if the seller and deliverer are assigned the same weighting, then if all other values are preserved across the two situations, the expected privacy violation will be the same. Thus, the critical difference in the results above arises from our first hypothesis that, because the seller is the least likely entity to incur trust, the seller

should know only the order information. In the next section, we describe the technologies needed for implementing the trust-enhanced models compared to those required for the traditional models.

6 Technology

In this section, we describe the technologies currently used to implement the proxy and no proxy models described earlier in this section and demonstrate that the proposed models can be implemented with the same technologies as the traditional models. These are:

Web Browser: A platform or application enabling a user to access and interact with web pages.

Web Server: A computer or application responsible for serving requests of a web browser.

Http: A request/response protocol between a web browser and a web server. Messages exchanged are in clear text and therefore vulnerable to eavesdroppers.

Digital Certificate: An electronic document which incorporates a digital signature to bind together a public key with an identity (information such as the name or address of a person or an organization).

Certificate Authority (CA): A trusted party responsible for issuing and signing digital certificates and for verifying their integrity.

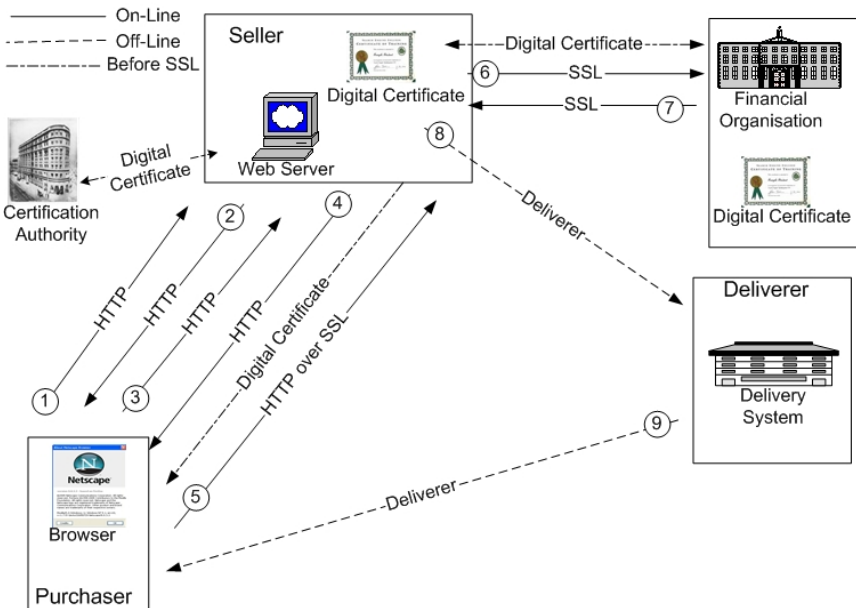


Fig. 2. Technologies used with the traditional protocol

Secure Socket Layer (SSL): A communication protocol which allows both participants to authenticate each other, while their communication is protected against eaves dropping.

Figure 2 illustrates the applications of the above technologies in the traditional model. Where proxies are used, for the sake of simplicity we identify them as appropriate with the associated entity (seller, deliverer or financial organization).

In considering the technologies needed for implementation of the trust-enhanced models proposed in section 3, we focus on model M4 as this is most similar to the traditional model because a single entity receives all personal information sent by the purchaser. Figure 3 below applies the same technologies in the M4 model, but in different ways. In Figure 3, the use of SSL between the web server and browser is the one critical addition enabling the privacy of information desired by the purchaser.

Figures 2 and 3 suggest that, in implementing M4, there need be no additional cost to the overall system, but that some cost is transferred from the seller to the deliverer. This is an acceptable cost, as the deliverer now has more opportunities for sales. On the other hand, the seller is in an improved situation, as there is no impact on their business, while their costs are, at the same time, reduced.

In an extended version of this paper, we give a detailed protocol implementing each of the four trust-enhanced models.

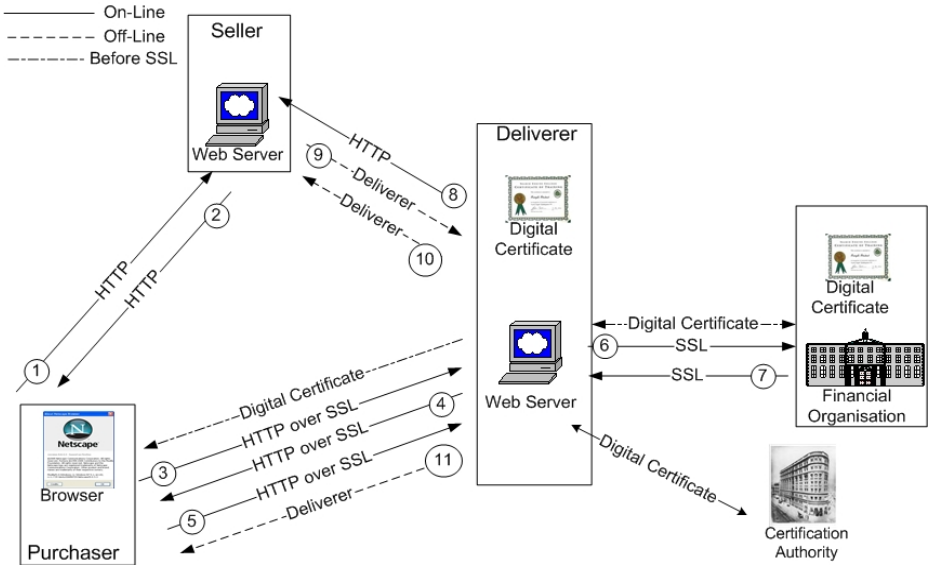


Fig. 3. Technologies used with the M4 model

7 Conclusions

In this paper, we introduce a measure of the trust based on the information distributed to the parties in an e-commerce transaction. Based on this precise method of

measurement, we are able to isolate the instances which maximize trust for the purchaser, leading us to propose four new models for e-commerce which improve consumer trust. Implementation of these new models in the e-commerce market place would therefore likely lead to an increase in on-line commerce. We describe in detail the technologies used to implement existing models and demonstrate that no new technologies are needed in order to implement the new models. The overall cost to the e-commerce system would remain the same while, internally, costs would be moved from the seller to the deliverer. An extended version of this paper, to be submitted elsewhere, will give detailed protocols for implementation of all four trust-enhanced models, along with proofs of security.

References

1. Al-Fedaghi, S.: How sensitive is your personal information? In: Proceedings of the 2007 ACM symposium on Applied computing, pp. 165–169 (2007)
2. Anderson, B.B., Hansen, J.V., Lowry, P.B., Summers, S.L.: The application of model checking for securing e-commerce transactions. *Communications of the ACM* 49, 97–101 (2006)
3. Barnard, L., Wesson, J.: A trust model for e-commerce in South Africa. In: Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, pp. 23–32 (2004)
4. Bhargav-Spantzel, A., Woo, J., Bertino, E.: Receipt management- Transaction history based trust establishment. In: Proceedings of the 2007 ACM workshop on Digital identity management, pp. 82–91 (2007)
5. Burns, S.: Unique characteristics of e-commerce technologies and their effects upon payment systems. GSEC (GIAC Security Essentials Certification)–Version 1 (2002)
6. Camenisch, J., Shelat, A., Sommer, D., Fischer-Hubner, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., Tseng, J.: Privacy and identity management for everyone. In: DIM 2005, pp. 20–27. ACM, Virginia (2005)
7. Chau, P.Y.K., Hu, P.J.H., Lee, B.L.P., Au, A.K.K.: Examining customers' trust in online vendors and their dropout decisions: An empirical study. *Electronic Commerce Research and Applications* 6, 171–182 (2007)
8. Claessens, J., Preneel, B., Vandewalle, J.: Anonymity controlled electronic payment systems. In: Proceedings of the 20th Symposium on Information Theory in the Benelux, pp. 109–116 (1999)
9. Doherty, S.: Keeping data private. *Network Computing* 12, 83–91 (2001)
10. Doney, P.M., Cannon, J.P.: An examination of the nature of trust in buyer–seller relationships. *Journal of Marketing* 61, 35–51 (1997)
11. Fomenko, V.: Generating virtual reality shops for e-commerce. Dissertation, Vrije Universiteit Brussel (2006)
12. Jarvenpaa, S.L., Tractinsky, N., Vitale, M.: Consumer trust in an Internet store. *Information Technology and Management* 1, 45–71 (2000)
13. Katsikas, S.K., Lopez, J., Pernul, G.: Trust, privacy and security in e-business: Requirements and solutions. In: Bozanis, P., Houstis, E.N. (eds.) PCI 2005. LNCS, vol. 3746, pp. 548–558. Springer, Heidelberg (2005)
14. Kumaraguru, P., Cranor, L.: Privacy in India: Attitudes and Awareness. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 243–258. Springer, Heidelberg (2006)

15. Moores, T.: Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM* 48, 86–91 (2005)
16. Seigneur, J.M., Jensen, C.D.: Trust enhanced ubiquitous payment without too much privacy loss. In: *Proceedings of the 2004 ACM symposium on Applied computing*, pp. 1593–1599 (2004)
17. Silience, E., Briggs, P., Harris, P., Fishwick, L.: A framework for understanding trust factors in web-based health advice. *International Journal of Human-Computer Studies* 64, 697–713 (2006)
18. Smith, L.M., Smith, J.L.: *Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?: American Accounting Association Southwest Region, Oklahoma City* (2006)
19. Tan, H., Guo, J.: Some methods to depress the risks of the online transactions. In: *Proceedings of the 7th international conference on Electronic commerce*, pp. 217–220 (2005)
20. Teo, T.S.H., Liu, J.: Consumer trust in e-commerce in the United States, Singapore and China. *Omega* 35, 22–38 (2007)
21. Tsiounis, Y.: A Security Framework for Card-Based Systems. In: *Proceedings of the 5th International Conference on Financial Cryptography*, pp. 210–231 (2002)