W3 Trust-Profiling Framework (W3TF) to Assess Trust and Transitivity of Trust of Web-Based Services in a Heterogeneous Web Environment

Yinan Yang[1], Lawrie Brown[1], Ed Lewis[1], and Jan Newmarch[2]

[1] School of IT&EE, UNSW@ADFA, Canberra, Australia
Yinan.Yang@act.gov.au, {l.brown, e.lewis}@adfa.edu.au
[2] School of Network Computing, Monash University, Melbourne, Australia
Jan.Newmarch@infotech.monash.edu.au

Abstract. The growth of eCommerce is being hampered by a lack of trust between providers and consumers of Web-based services. While researchers in many disciplines have addressed Web trust issues, a comprehensive approach has yet to be established. This paper proposes a conceptual trust-profiling framework through a range of new user-centred trust measures. W3TF is a generic form of trust assessment that can help build user confidence in an eCommerce environment. It incorporates existing measures of trust (such as Public Key Infrastructure), takes account of consumer perceptions by identifying trust attributes, and uses Web technology (in the form of metadata), to create a practical, flexible and comprehensive approach to trust assessment.

1 Introduction

The meaning of trust in the context of eCommerce is still evolving, along with the Web environment and technologies [3, 11, 13, 14]. Traditional trust relationships between business parties are based on legitimate physical identities such as a shopfront or business premises. This physical manifestation is in contrast to the eCommerce environment of the Web, where business providers and consumers identify each other by some electronic means such as their websites, email addresses, a public key or certificate.

Recent surveys have shown that one of the biggest concerns for Internet consumers (Web users) is a lack of trust in websites [9, 1]. Many researchers identify the credibility of a website as a very important factor that consists of two key components: *Trustworthiness* and *Expertise* [4, 5]. The first dimension of credibility is defined by the terms well-intentioned, truthful, unbiased, and so on; capturing the perceived goodness or morality of the sources. The other dimension of credibility is defined by terms such as knowledgeable, experienced, or competent; capturing the perceived knowledge and skill of the source. Shneiderman et al, identified two principles and associated guidelines to enhance cooperative behaviours and to win user/customer loyalty [17]. A number of trust factors were identified, such as assurances, references, certifications from third parties, and guarantees of privacy and security. These identified trust factors are also more or less agreed among researchers of empirical trust studies and surveys [2, 7, 16].

X. Zhou et al. (Eds.): APWeb 2006, LNCS 3841, pp. 367 – 378, 2006.

These concerns have been addressed using different approaches by Jøsang et al [12] who focused on a particular mathematical modeling approach to trust, and recently by Herzberg and Jbara [8] who also focused on a practical technique for presenting a trust measure in a user's web browser.

Electronic (Digital) security technology plays an important role in establishing trust in an eCommerce environment [12]. It also provides a tangible perception of trust for online consumers. From the viewpoint of security communities, online trust can be secured through public-key cryptography, which has been used for anti-spoofing, authentication, authorisation, non-repudiation, and secure data communications. The major PKI models adopted by industry are primarily hierarchically structured to form a vertical trust environment [18]. However, the Web provides an unrestricted or unlimited number of hypertext links (that is, hyperlinked webdocuments) to form a horizontal referral environment. The combination of horizontal and vertical environments gives rise to a heterogeneous environment. Measurement of trust in this heterogeneous environment requires a different approach from those already established [6, 10]. These distinguishing characteristics of the general operation of eCommerce pose a challenge for online consumers to gather sufficient information in a heterogeneous environment on which to base trust assessments.

The novel contribution of this paper is to develop a generic trust-profiling framework to assess the trustworthiness of webdocument(s). It will do this by translating identified trust criteria into trust metadata that are assigned to proposed trust categories and trust domains, which can then be evaluated using various calculations, and the result distributed to Web users or other applications or trust systems.

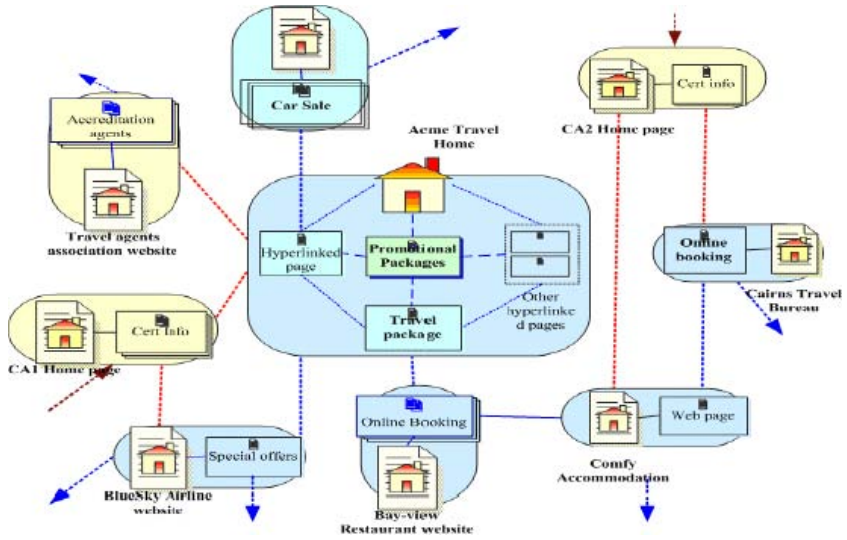

Fig. 1. Hypothetical ACME Travel online-service provider's operational environment

We then present an example application of the proposed W3 trust-profiling framework for the fictitious Acme Travel, who promote their holiday packages on the Web (Figure 1). Its webdocuments have a number of external hyperlinks to other business partners, professional associations and certificate authorities, and its website is referenced by peer professional associations and certificate authorities, as evidence of its validity.

2 Brief Description of the W3TF

The proposed Web trust-profiling framework (W3TF) is a generic trust-profiling framework for evaluating the trust and transitivity of trust of online services in a heterogeneous environment [19], where *Transitivity of Trust* concerns how the trust value of a webdocument can influence or be influenced by another hyperlinked webdocument (or nodes).

It proposes two main trust assessments, *standalone* and *hyperlinked* trust assessments, based on different types of webdocument content and relationships, as illustrated in the Acme Travel example.

All hyperlinked webdocuments combine a horizontal Web referral environment and a hierarchical PKI environment to form the heterogeneous environment identified by W3TF. Each trust assessment has a number of components and is based on various types of trust information, which can be extracted from various sources and then classified into various trust categories. Trust assessments are then carried out using the various trust categories with their associated trust domains. Trust information is represented by a proposed initial set of trust metadata [20].

Figure 2 is a diagrammatic conceptual view of the proposed W3 trust-profiling framework.

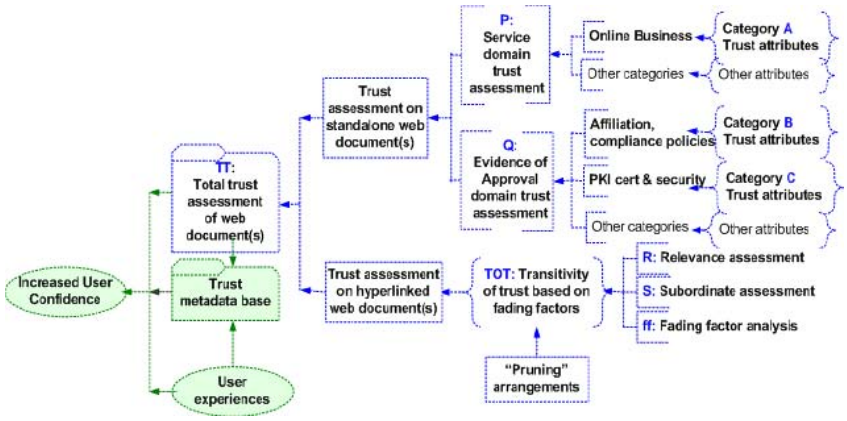

Fig. 2. Conceptualised trust-profiling framework of W3TF

A website may have arbitrary number of standalone webdocuments and external hyperlinks. The service provider, its business associates and partners can alter their webcontents, and hyperlinks to other webdocuments, at will. Hence, there is very

little restriction on, or standards for, the changes that service providers can make to their webdocuments. In the W3TF, all internal hyperlinks and webdocuments sharing the same DNS name are known as 'standalone webdocuments'; all external hyperlinks and associated webdocuments residing on different websites are considered as 'hyperlinked webdocuments'. The trust profile of a webdocument is the result of a combination of both standalone and hyperlinked trust assessments, which can be stored in a trust database for future reference.

3 Trust Assessment on Standalone Webdocument

Standalone trust assessment is the analysis of the trust information in a webdocument without considering hyperlinks and hyperlinked webdocuments and their webcontents. Before trust assessment starts, necessary trust information is extracted and categorised into predefined trust categories for 'cross-examining' against trust criteria in each trust category [21].

Standalone trust assessment is carried out based on the following initial three trust categories:

- Category A relates to the contents of the webdocument that provide information about an online service provider and their business. This self-declared information is placed in a webdocument by individual providers and might include details about primary and secondary businesses and contact information. Possible sources of information include the HTML document contents and HTTP protocol metadata.
- Category B relates to affiliation and compliance such as membership of business and professional associations, reputation, policies, and legal status, which can be sourced from a third party. Each claim must be verified with peak bodies or a trusted third party.
- Category C relates to relationships between an online service provider and a PKI certificate (PKI cert) authority. Each PKI cert must be verified with the PKI certificate issuer that is a third party.

Category A metadata becomes part of the *online-service Web referral trust domain*. Metadata for categories B and C are classified in the *evidence-of-approval trust domain*. The collective trust values of the metadata of each category represent the overall trust value of a webdocument in a heterogeneous Web environment. Trust assessment on a standalone webdocument is based on a parallel assessment of both trust domains, as shown in Figure 2.

The number of categories can be extended to incorporate other forms of trust information as required. Each trust category comprises a number of trust attributes and each attribute is represented by certain trust metadata.

One way to assess the level of trust (or relative degree) of the overall trust value of a webdocument is by using the trust weighting of the proposed trust metadata through the contribution from each trust category. Each trust category has a set of predefined trust attributes. A trust attribute acts as an atom of trust. Each trust attribute carries some 'weight' of trust value, which allows interpretation of the trust perspective of a webdocument.

The trust value is weighed from each trust attribute of the category with a consideration given to elements of uncertainty. Then the collective trust value of each category contributes to the overall trust value. However, before applying any theories and formulae, each trust assessment component must be formalised and their interrelationships denoted in a symbolic and generic form, to which various calculations can then be applied for weighing trust attributes and estimating a trust value of webdocuments. The collective trust weights of each of the categories A, B and C are combined to contribute to the overall trust value of the targeted webdocument.

4 Transitivity of Trust

In the hyperlinked web referral environment, transitivity of trust is the central thread in trust assessments [22]. It concerns the extent to which the trust value of a webdocument influences or is affected by hyperlinked webdocuments (or nodes). The purpose of transitivity of trust is to achieve scalable trust, which allows a certain level of trust to travel to a number of nodes (or entities) and still be able to maintain that level of trust in a specific time frame.

Transitivity of trust assessment is to ensure (or maintain) the measurement of a trust relationship among the maximum number of hyperlinked webdocuments by identifying any *penalty factors* in the online-service Web referral environment, e.g. online service spam behaviour. Each hyperlink and hyperlinked webdocument must be able to demonstrate a need (or justification) for the existence of a relationship between the targeted webdocument and the hyperlinked webdocument.

Transitivity of trust assessment includes *relevanc*e assessment and *subordinate assessment*, which examine different *penalty factors* and *fading factors* in different trust domains of the hyperlinked webdocuments. As part of a transitivity of trust assessment, pruning is used to reduce unrestricted hyperlinked webdocuments to a manageable size using relevance assessment to arrive a relevant tree, on which a trust profile of the targeted webdocument can be based.

The proposed method of evaluating trust for hyperlinked webdocuments uses a transitivity of trust assessment that includes:

- relevance assessment: of the business relationship between two hyperlinked webdocuments;
- subordinate assessment: of the trust implications and the influence of hyperlinked webdocuments;
- fading (and penalty) factor analysis: of elements that will reduce online trust as it travels between hyperlinked webdocuments; and
- pruning arrangements in the web referral environment: of possible ways to ensure a reasonable and manageable sized tree for real-time trust assessment.

All hyperlinked webdocuments belonging to other websites will be assessed in hyperlinked trust assessments.

4.1 Relevance Assessment

Relevance assessment analyses evidence of business relationships between hyperlinked webdocuments to ensure the purpose of this business relationship is to fulfill business requirements. Relevance assessment measures the relevance of online service(s) between the targeted webdocument and a hyperlinked webdocument. The targeted webdocument's primary service could act as a benchmark for other hyperlinked webdocuments to compare or match up with, thereby providing an indication of whether there is a relevance relationship between the targeted webdocument and the hyperlinked webdocument.

Relevance assessment serves two purposes. First, it ensures all hyperlinked webdocuments have some kind of relevance relationship with the targeted webdocument in the online-service domain. Second, it provides a mechanism to prune down the number of hyperlinked webdocuments to a more manageable size according to the requirements or definition of the online-service domain. The result of this process is described as a *relevance tree*.

In a relevance tree, each node is considered as both standalone and hyperlinked to the 'targeted' node, unless the relevance tree has only one node. So trust evaluation is based on a standalone assessment followed by a hyperlinked assessment. In a relevance tree, all nodes except the targeted webdocument (node) are labelled as hyperlinked webdocuments with a relevance relationship with the targeted webdocument and so labelled as subordinate nodes of the targeted notes. Subordinate assessment provides additional trust evaluations for hyperlinked webdocuments. These assessments can be used to analyse the transitivity of trust and demonstrate the influence of hyperlinked webcontents on the trust value of a webdocument.

4.2 Penalty and Fading Factor Analysis

The role of penalty or fading factor analysis is to examine elements of uncertainty in each trust domain. These elements of uncertainty can be seen as potential barriers for achieving scalable trust in a heterogeneous Web environment. A number of uncertainty elements in each domain, both tangible (i.e. facts) and intangible (such as user confidence based on practical experience or perceptions), can be identified. These elements of uncertainty are defined as *penalty factors* for the online-service Web referral trust domain; and as *fading factors* for the evidence-of-approval trust domain. Both factors can reduce the weight of trust during trust and transitivity of trust assessment.

Penalty factors for the online-service domain are determined through relevance assessment of the Primary Service between the targeted webdocument and its hyperlinked webdocuments. If the degree of relevance is less than, say, 50% then the hyperlinked webdocument is tagged as irrelevant and the targeted page will be recorded as having a penalty factor. If a targeted webdocument has more irrelevant links, then it will have more penalty factors. This penalty will reduce the trust value of Category A of the targeted webdocument. The trust value of Category A will contribute to the overall trust value of the webdocument. The trust value of each node in the relevance tree will then influence or determine the trust value of the targeted webdocument. So the more penalty factors in Category A, the lower the trust value of the category.

The fading factor analysis in Category B is based on the result of verification of each claim that is linked to a trusted third party (TTP). Additional fading factors are accumulated by each negative verification result—either unverifiable claims or false claims—in the trust category. So the more fading factors in Category B, the lower the trust value of the category.

In Category C, fading factor analysis is based on the length of the hierarchical certification path to reach the root certificate authority (CA). The root CA is the most trustworthy during the certification process according to the X.509 PKI standard [18].

At the end of the verification and validation processes, 'approval-trees' (for example, a number of hops to the trusted third party in Category B; the number of entities in a chain of certificates for Category C) will be constructed. These trees are used for calculating fading factors in each category. The more hops, the more fading factors will be accumulated. However, in practice, there is often a direct hyperlink (or single step) between the subject webpage and the trusted third party website to verify professional affiliation in Category B; the same frequently applies for the PKI chain of trust in Category C.

This 'fading factor' by back-propagation, as mentioned in [15], led to the proposed W3 trust-profiling framework. However, the W3TF has consolidated and extended the use of the factor through the new concept of transitivity of trust in trust domains and essential trust evaluation processes.

4.3 Subordinate Assessment

The proposed subordinate assessment analyses the trust implications and influence of hyperlinked webdocument(s). In a relevance tree, each webdocument (that is, node) often has hyperlinked webdocuments. These hyperlinked webdocuments could be described as 'child' (or subordinate) nodes of the parent node. A webdocument may have a number of child nodes, which also have their own child nodes, which can be treated as 'grandchild' nodes. The structure of family generation (that is, the parent, children and grandchildren) is used to express the tree structure of hyperlinked pages in a trust domain. Subordinate assessment analyses how each hyperlinked webdocument's trust value affects its parent node, hence, the overall trust value of the targeted webdocument. This analysis will be incorporated into a tree pruning process, such as depth-bounded/ breadth-bounded pruning techniques.

4.4 Total Trust Assessment

Total trust assessment combines the trust values of all hyperlinked webdocuments in the relevance tree. It is a recursive process. Each hyperlinked webdocument in the relevance tree is cross-examined by both standalone and hyperlinked trust assessments. This process is repeated until all hyperlinked nodes in the original relevance tree have been examined.

An initial trust profile is the result of a total trust assessment of a webdocument when performed for the very first time. This initial trust profile can be stored in a trust profile database for future reference. The total trust assessment of the targeted webdocument is based on combining the trust assessments of standalone webdocuments residing on the same website (Category A, B, C of each

webdocument) and hyperlinked webdocuments (with the associated subordinate nodes) in the relevance tree, and normalising the result. In other words, the result of the total trust assessment is not only based on the standalone web document's trust assessment, but also takes account of the subordinate assessment of all hyperlinked webdocuments.

5 Illustrative Example of a W3TF Transitivity of Trust Evaluation

In a heterogeneous web environment, the trust-profiling process starts with identifying the targeted webdocument on a website where a trust profile is required, along with webdocuments that are hyperlinked to the starting point. Acme Travel's trust profile is based on trust assessments of the targeted webdocument as well as of BlueSky Airline, Bayview Restaurant, Comfy Accommodation and Cairns Travel Bureau webdocuments (Figure 1). After the relevance assessment is carried out on all hyperlinked webdocuments starting on Acme Travel's targeted webdocument, a relevance tree is generated from a graph of all hyperlinked webdocuments. Based on this relevance tree (Figure 3), each node is subjected to standalone trust assessment and subordinate assessment. The result of recursive trust assessment is the trust profile of Acme Travel.

The proposed W3TF evaluation process is a recursive one, which combines standalone and hyperlinked trust assessments on a webdocument and its hyperlinked webdocuments. After the standalone trust assessment is done on the trust categories of a webdocument, transitivity of trust is assessed on hyperlinked webdocuments according to different types of inter-relationships. The result of both trust assessments is the trust profile of the webdocument for which a trust assessment was required.

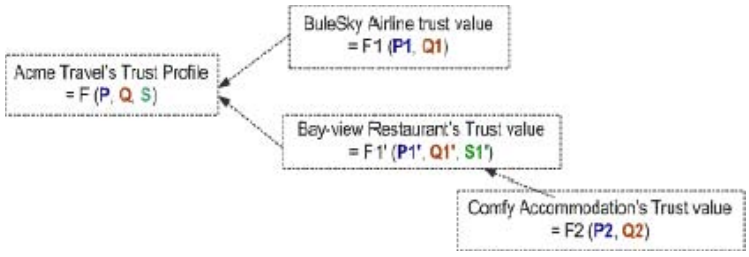

Fig. 3. Symbolic notation of the relevance tree of Acme Travel

The evaluation process thus combines the following elements used in the standalone and the hyperlinked trust assessments. To apply a mathematical formula for weighing and combining trust values for trust-profiling evaluation [22], a symbolic notation is necessary (Figure 3). The results of this assessment are summarised in Table 1.

P represents the trust assessment resulting from the combination of values of the trust metadata in category A of the online-service domain of a standalone webdocument.

In generic terms, a suitable value of P can be obtained from a function based on the number of attributes present:

- Count the number of attributes present; for example, 5
- Divide by the total number of attributes in Category A; that is, 5/16
- Assign the above calculation result to P value; that is, P = 0.3125

Based on this, and on hypothesized page contents for each (see [19]), P values for Comfy, Bayview, BlueSky and Acme are 0.9375, 1, 0.9375 and 0.6 respectively.

Q represents the trust assessment resulting from the combination of professional affiliations (Category B) and a chain of certificates (Category C); that is, the result of verification of the evidence-of-approval domain. Including consideration of the fading factors, Q values for Comfy, Bayview, BlueSky and Acme are 0.7, 0.7, 0.8 and 0.8 respectively.

R represents the relevance assessment resulting from the measurement of the relevance of online service(s) between a hyperlinked webdocument with the targeted webdocument. The target Acme webdocument has a default R value of 1. For the other pages, key Category A attributes (for example, Primary-Service) are compared with the target webdocument to determine their degree of relevance. This comparison gives R values for Comfy, Bayview, and BlueSky of 0.5, 1.0, 0.6 respectively.

S represents the results of subordinate assessment, which is based on trust assessment of other standalone webdocument(s) in the relevance tree. A standalone webdocument (e.g. the targeted webdocument) often has hyperlinks to other webdocument(s), each of which has a relevant trust value of S1, S2… Sn. That is, S = s (S1, S2, …, Sn) where Si = s (TTi, Ri) for some functions (see description of TT below). S is the contribution to this document from children's total trust value and associated relevance-value (R) in the relevance tree. In general, S is the sum of the combination of the total trust value of child nodes (TT-child) and the relevance values (R-child) of direct-subordinate nodes; that is,

$$Si = s(TT, R) = \sum (TT\_child \times R\_child) / \text{no. of children}) .$$

If there is no child node, then S = 0, being a special case for leaf nodes of a tree. Based on this, S values for Bayview and Acme are 0.2895 and 0.4519.

TOT represents the assessment of transitivity of trust, which concerns how the trust value of a webdocument is influenced or affected by hyperlinked webdocuments. It is desirable to be able to achieve scalable trust on the Web, which allows a certain level of trust to travel to a number of nodes (or entities) and still be able to maintain a certain level of trust within specific period.

TT denotes the result of overall trust assessment of a webdocument. It combines the values of categories A, B, C of the standalone webdocument and associated subordinate nodes in the relevance tree and normalises the result. TT can be measured through a number of possible ways, which include extracting trust attributes, weighing each trust category and combining the result of all trust assessment components including P, Q and S for each webdocument. TT is required for every node in a relevant tree. In generic terms, a value of TT can be obtained from a function based on the total trust value of each hyperlinked webpage, which can be expressed in the following way: TT = tt (P, Q, S). For a leaf node with no hyperlinked child node, TT = tt (P, Q). Computing TT is a recursive process. The TT

of Acme value is based on each total trust value of each node in the relevance tree (Figure 3). The following formula is used for the TT value: TT = (P, Q, S) = (P + Q + S) / 3, so

TT of Comfy = (0.9375 + 0.8 + 0) / 3 = 0.579

TT of Bayview = (1 + 0.35 + 0.2895) / 3 = 0.5465

TT of BlueSky = (0.9375 + 0.85 + 0) / 3 = 0.5958

TT of Acme = (0.6 + 0.85 + 0.4519) / 3 = 0.7666

That is, the total value of the targeted page Acme is 75.06% as shown in Table 1.

Table 1. Total Trust calculation of Acme

Node ID	P	Q		R	S	TT
	Cat-A	Cat--B	Cat-C			
Comfy	0.9375	0.7	0.9	0.5	0	0.579
Bayview	1	0.7	0	1	0.2895	0.5465
BlueSky	0.9375	0.8	0.9	0.6	0	0.5958
Acme	0.6	0.8	0.9	1	0.4519	0.766

The total trust value of Acme's holiday package webpage, is 76%, which combines the values of two domains including associated fading factors, with the standalone trust value of the subordinate value of the relevance tree. The results can either be self stored or stored at a third party's trust database for historical information, and displayed to end users through a front-end client interface

In brief, the proposed trust evaluation model performs the following functions in different components:

1. Input component: identifies sources of trust information, assigns the default weight for each trust attribute according to its category and draws a graph by following each external hyperlink from Category A of the targeted webpage, Acme;
2. Trust metadata construction component: constructs the relevance tree based on relevance assessment (i.e. assessing fading factors) according to the Primary Service of Category A of Acme;
3. Trust evaluation component: calculates P, Q, S and TT values including fading factors in Categories B and C of each node in the relevance tree;
4. Trust metadata reconstruction component: updates the trust metadatabase with associated trust profiles for future reference; and
5. Output component: prepares different formats of the total trust value of the targeted webpage, Acme, which can be read either by devices or Web users.

Full details of the trust evaluation and possible formulae are provided in [19].

6 Conclusion

The proposed W3 trust-profiling framework (W3TF) combines efforts by Web research communities with associated issues from the wider Web trust spectrum,

including government and industry, to present a promising approach for online trust assessment and a sound foundation from which further studies might be built.

The W3TF is versatile. It can be expanded to accommodate new trust attributes, categories and domains, and trust can be 'weighed' (and therefore evaluated) by using various mathematical formulae based on different theories and policies.

Clearly further work is required to validate the practical implementation of this framework. This work would involve deploying a prototype implementation of the framework, investigating other possible sources of trust attributes, and evaluating various models for combining the trust attributes into a final overall value.

In a heterogeneous Web environment, transitivity of trust can be achieved through a combination of standalone and hyperlinked trust assessments and appropriately constructed relevance tree. W3TF provides a mechanism for the evaluation of trust and transitivity of trust through trust metadata and associated trust categories, relevance assessment, subordinate assessment, fading factor analysis, trust weighting to allow evaluation of different trust domains. Based on this trust profile, we believe that online consumers can make a more informed decision, and consequently, their user confidence would be improved.

References

[1] France Belanger, Varadharajan Sridhar, & Craig Van Slyke. *Comparing the Influence of Perceived Innovation Characteristics and Trustworthiness Across Countries*, Proceeding of the International Conference on Electronic Commerce Research (ICECR-5), Nov 2002

[2] Cheskin & Studio Archetype/Sapient, San Francisco*, eCommerce Trust Study,* Jan 1999. www.cheskin.com/think/studies/ecomtrust.html

[3] iTrust, *Aspects of Trust*, The iTrust working group, http://www.itrust.uoc.gr /dyncat.cfm?catid=37, cited 28 Oct 2005

[4] B. Fogg, J. Marshall, O. Laraki, A. Osipovich, C. Varma, N. Fang, J. Paul, A. Rangnekar, J. Shon, P. Swani, M. Treinen. *What Makes Web Sites Credible? A Report on a Large Quantitative Study.* Proceedings of the SIGCHI Conference on Human factors in Computing Systems, Seattle, USA, pp 61-68. 2001. ISBN:1581133278.

[5] BJ Fogg, Jonathan Marshall, Tarmi Karmeda, Joshua Solornon, Akshay Rangnekar, John Boyd, & Bonny Brown. *Web Credibility Research: a Method for Online Experiments and Early Study Results,* 2001. http://www.webcredibility.org/studies/WebCred Fogg CHI 2001 short paper.PDF

[6] Gorsch, D. *Internet Limitations, Product Types, and the Future of Electronic Retailing*. Proceeding of the 1st Nordic Workshop on Electronic Commerce, Halmstad University: Viktoria Institute, May 2001.

[7] T. Grandison and M. Sloman. *A Survey of Trust in Internet Applications*, IEEE Communications Surveys and Tutorials, Fourth Quarter 2000, Vol 3, No 4, IEEE www.comsoc.org/livepubs/surveys/public/2000/dec/grandison.html.

[8] Amir Herzberg and Ahmad Jbara, *Reestablishing Trust In the Web*, Dr. Dobb's Journal, Oct 2005

[9] Donna L. Hoffman, Thomas P. Novak, Marcos Peralta. *Building Consumer Trust Online.* Communications of ACM, Vol 42, No 4, pp 80-85, Apr 1999. ISSN: 0001-0782.

[10] Head, M.M., Yuan, Y., Archer, N. *Building Trust in E-Commerce: A Theoretical Framework*. Proceeding of the Second World Congress on the Management of Electronic Commerce, MCB Press, Jan 2001.

[11] S. Jones. *TRUST-EC: Requirements for Trust and Confidence in E-Commerce*, Workshop Requirements for trust and confidence in E-commerce, Luxembourg, CEC, 1999.

[12] Audun Jøsang, Ingar Glenn Pedersen and Dean Povey. *PKI Seeks a Trusting Relationship*, In Ed Dawson, Andrew Clark, Colin Boyd (eds), Information Security and Privacy: Proceedings of ACISP 2000, Lecture Notes in Computer Science, Vol 1841, pp191-205, Springer-Verlag, 2000. http://security.dstc.edu.au/papers/pkitrust.pdf

[13] Peter Keen. *Electronic Commerce and the Concept of Trust*, 1999. http://www.peterkeen.com/recent/books/extracts/ecr1.htm, cited 28 Oct 2005

[14] Luis F. Luna-Reyes, Anthony M. Cresswell, George P. Richardson. *Knowledge and the Development of Interpersonal Trust: a Dynamic Model.* Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS '04) – Track 3, p30086a, 2004.

[15] Massimo Marchiori, *The limits of Web metadata, and beyond,* The World Wide Web Consortium (W3C), MIT Laboratory for Computer Science, USA, 1998. http://www7.scu.edu.au/programme/fullpapers/1896/com1896.htm

[16] Princeton Survey Research Associates. *A Matter of Trust: What Users Want From Web sites*, Jan 2002. http://www.consumerwebwatch.org/news/report1.pdf

[17] Ben Shneiderman. *Designing trust into Online Experiences*, Communications of the ACM, Vol 43. No 12, pp57-59, Dec 2000. ISSN:0001-0782.

[18] ITU-T Recommendation X.509, *Information Technology - Open Systems Interconnection - the Directory: Authentication Framework,* International Telecommunication Union, Jun 1997. ISBN: 0733704263.

[19] Yinan Yang, *W3 Trust-Profiling Framework (W3TF) to assess Trust and Transitivity of trust of Web-based services in a heterogeneous Web environment*, PhD Thesis, School of Information Technology and Electrical Engineering, University of New South Wales, ADFA, Canberra, Australia, Aug 2004.

[20] Y. Yang, L. Brown, J. Newmarch and E. Lewis, *Trust Metadata: Enabling Trust and a Counterweight to Risks of E-Commerce*, Proceedings Asia Pacific World Wide Web Conference, p197-203, 1999.

[21] Y. Yang, L. Brown, J. Newmarch, E. Lewis, *A Trusted W3 Model: Transitivity of Trust in a Heterogeneous Web Environment*, Proceedings of the Fifth Australian World Wide Web Conference, Queensland, pp59-73, Apr 1999. ISBN:1863844554.

[22] Y. Yang, L. Brown, E. Lewis, and J. Newmarch. *W3 Trust Model: a Way to Evaluate Trust and Transitivity of Trust of Online Services*, Proceedings Internet Computing Conference, Las Vegas, USA, Jun 2002.