W3 Trust Model:
Evaluating Trust and Transitivity of Trust of Online Services

Yinan Yang
The Department of Urban Services
ACT Government, Canberra, ACT Australia

Dr Lawrie Brown
School of Computer Science
University of New South Wales, University College, ADFA, ACT Australia

Dr Edward Lewis
School of Computer Science
University of New South Wales, University College, ADFA, ACT Australia

A/ Prof Dr Jan Newmarch
School of Network Computing
Monash University, Melbourne, Vic Australia

Abstract: *By introducing a set of trust attributes, the proposed W3 Trust Model combines a vertically trusted public key infrastructure with a horizontal referral Web classification. It provides a mechanism to assess both the trust and the transitivity of trust of web contents in a heterogeneous environment.*

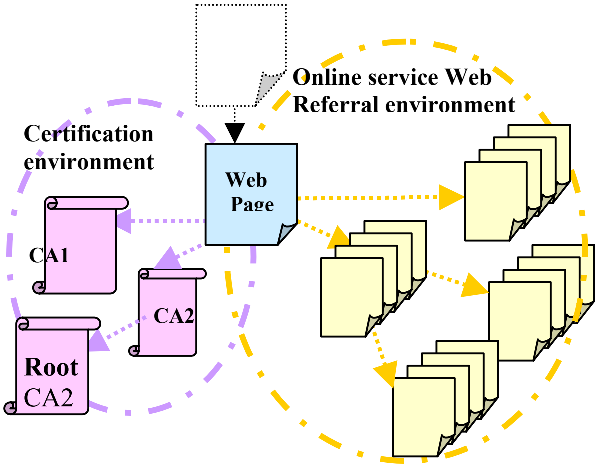
Keywords: trust metadata, trust, transitivity of trust, eCommerce.

1. Introduction

The proposed W3 Trust Model (W3TM) is a way to address an important question: how to measure the trust worthiness of online services through evaluating the trust and transitivity of trust of Web contents? The W3 Trust Model [1] brings the concepts of trust and transitivity of trust into an analysis of front-end Web contents using a proposed trust evaluation process framework.

We have previously proposed a set of trust metadata [2] to help assess the trustworthiness of Web contents within a heterogeneous environment using the W3 Trust Model. This paper provides a brief description of how the W3 Trust Model works; looks into each component of trust assessment of the W3 Trust Model with associated design choices and techniques; and follows up with a simple example to illustrate trust evaluation in an online service.

Figure 1 is an overview of the trust evaluation environments of the W3 Trust Model. The "Web Page" represents an online service provider's Web page and it is the starting point in the graph where trust value evaluation is required.


Online service Web Referral environment
Certification environment
Web Page
CA1
CA2
Root CA2

(Figure 1) Overview of the trust evaluation environments of the W3TM

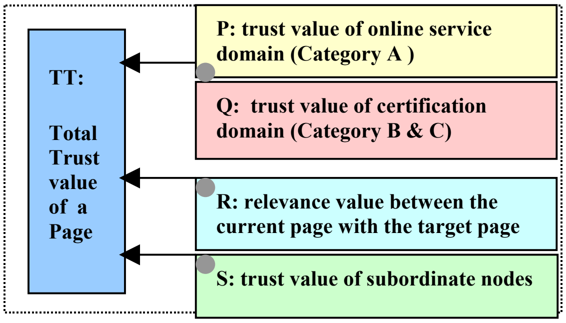
In brief, the total trust (TT) value of a targeted site is based on the result of recursive calculation of the following component assessments(Figure 2):

- Standalone page trust assessment. The values of calculation on "standalone assessment" are denoted as P for the service domain (ie. category A) and Q for the certification domain (ie. category B and C).
- "Relevance assessment" among hyperlinked pages. The value of calculation of "relevance assessment" is denoted as R.

- Subordinate node assessment. The sum of "total trust" and "relevance" assessments of hyperlinked pages (ie. child nodes) in the online service Web referral domain. The value of the calculation of this subordinate assessment is denoted as *S*.

In other words, TT is the combination of the P value of the page, the S values (including associated R values), and the Q value for the certification domain. Total trust value of a targeted page is a combination of values of two domains including associated fading factors, the standalone-trust-value of the subordinate-value of the relevance tree:

- P: Trust-value = combination of values of the trust metadata categories A
- Q: Trust-value = the result of verification of the certification domain (ie. the category B and C)
- S: Subordinate-value = contribution to this page from children's total trust value and associated relevance-value (R) in the relevance-tree.


TT:
Total Trust value of a Page
P: trust value of online service domain (Category A)
Q: trust value of certification domain (Category B & C)
R: relevance value between the current page with the target page
S: trust value of subordinate nodes

(FIGURE 2) W3TM Assessment components

It is necessary to examine each component in terms of general concepts, calculation restrictions, possible mathematical formulae, illustrative examples and some associated issues.

2. Standalone trust assessment

Standalone trust assessment indicates the trust analysis of a single page on a site. It does not analyse any contents of hyperlinked sites. Based on a standalone web page's content, trust assessment can be made by analysing three categories of trust metadata : Category A is the self-description of its own Web content; Category B is the description of affiliation, compliance (ie. the relationship-description of the Web site with others); and Category C is the description of certification (see [2] for details). These three categories of trust attributes are the building blocks of the W3 Trust Model and describe two environments in which an online service operates. Category A provides descriptive information about the online service Web referral environment. Category B provides descriptive information about association, reputation, policies, and legal requirements. Category C provides the Public Key Infrastructure (PKI) certification environment. These three categories also are classified into two domains in the trust evaluation process framework. In other words, the standalone trust assessment is based on a parallel assessment of both domains; that is, the online service domain (P domain: category A) and the certification domain (Q domain: category B and C).

3. Online Service Domain

P is a numeric value derived from the trust metadata category A of a web page (standalone page) that represents the trust value of the service domain of the page. It looks at content such as metadata for keywords, but does not follow any hyperlinks. The value of P is calculated through a number of trust attributes of Category A. The presence or absence of these attributes in Category A determines the P value of the page. Following is an example formula:

$$P = \frac{\text{Number of attributes present}}{\text{Total number of attributes in Category A}}$$

For example, a page U has five attributes of the sixteen defined in Category A: Title, Keywords, Rights Publisher and Org-type. Using the above formula, then the value is: P = 5/16 =0.31.

More work needs to be done in how the total number of attributes is determined through a semantic analysis.

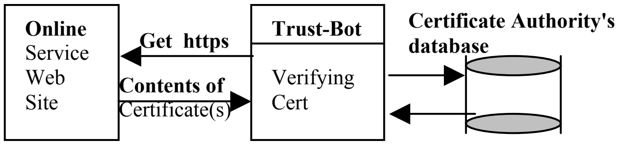
4. Certification Domain

Q is a numeric value that is derived from combination of professional affiliations (Category B) and a chain of certificates (Category C). Verification is required for all claims in the Q domain. Each attribute in the category B and C must be verified. Any false claim or absent attributes in either category will reduce the associated category's trust value. There is a "fading factor" [3] associated with both Category B and C.

In Category B, attributes provide descriptive information in the areas of affiliation, reputation, policies and legal requirements. Each attribute must be verified, such as Professional-affiliations, External references, Customer protection policies and Services awards.

In Category C, a chain of certificates (ie. a special case of tree) is also known as “a chain of trust” in the X.509 standard [4]. To construct a "valid certificate chain", a verification or confirmation process must be carried out for each “certification path" to its root certification authority. There are 5 attributes (eg. certificate-Owner and Validity-period) for each certificate that must be verified to validate a certificate. For each valid certificate, a chain of trust (path to its root) to its issuer is constructed. In principle, the longer the path to the root CA, the more "fading factors" are accumulated. Each certificate carries a certain weight of trust value. This trust value will only be counted if the result of verification/checking is a positive result. A certificate seal (ie. gif file) on a web site has no real trust value according to the W3 Trust Model. The validity check can be performed by matching certificate information on both sites, ie. the certificate issuer’s and the online service sites.

The positive and negative results of the verification process are used to calculate the category trust value. This verification process could be done automatically with the Trust-Bot (Figure 3) - a trust evaluation engine using the W3 Trust Model.



(Figure 3) Verification process by the Trust-Bot

The following is a method to calculate the Q value. For Category B, each attribute must be verified and add all positive results or deduct any false claim. For Category C, a similar process as calculation of Category B is carried out.

- Verifying each certificate information with the issuer site. The trust value should be decreased by non-confirmative/unverifiable claims if a maximum-trust model is used initially. A maximum-trust model [3] sets the initial total trust value to 100% and then subtracting trust values from it according to the collected trust attributes. Otherwise, increase trust value if a zero-trust model [3] used as default. A zero-trust model sets the initial total trust value to 0% and then adding trust values to it according to the collected trust attributes.
- CAs reputations and length of path to the root CA determine trust weight and vary the value of Q. For example, a well-known CA carries a high trust rating; an unknown CA carries less trust rating; the longer the chain of certificates, the more cumulative “fading factors”.

There are some conditions or restrictions on Category A (P value), B and C (Q value). They must be between 0 and 1. If one page U1 has a superset of attributes to another page U2, then the P value for U1 is higher than the P value for U2. That is, the more attributes, the better the P value.

By the same principle, if one page U1 has positive results of claims (Category B) and a valid PKI certificate (Category C) and other page U2 does not, then the combination of Q value for U1 is higher than the Q value for U2. Having a valid PKI certificate improves the Category C value.

The standalone trust value of each page will be carried out only on sites with unique domain name spaces. The issue of evaluating each page residing in the same domain space will be carried out in future work.

5. Relevance Assessments

The relevance assessment is measuring "relevance" of online service(s) between a hyperlinked site with the targeted site. The result of this assessment is denoted as R.

Each site has the attribute of "primary service" in Category A. The targeted site's primary service acts as a benchmark for other sites to match up with. General rules are:

- If the targeted site has defined a number of service(s) (eg. dating service, restaurant, and hotel) and type of hyperlinks belongs to the category A (denoted as Cat-A external to/from links in W3TM), then each hyperlink site shall be assessed for "relevance". It could be done by comparing primary service(s) attribute in the category A of both sites.
- If a hyperlinked site's primary service attribute of Category A is a subset of a primary service attribute of the targeted site, then this hyperlinked site can be tagged as a "relevant site".
- Each hyperlinked site must be identified by a unique domain name. This is to ensure that relevance assessment is only on unique (ie. different) online service provider's Web sites.

However, there are a number of methods for relevance assessment. Some existing Internet search technologies [6, 7] and algorithms on "relevance" can be utilised, such as WAIS, Connectivity-based ranking and hyperlink analysis [8]. Some indicators of "relevance" and measuring techniques can be used:

- *Reversed hyperlink*: not only the targeted site has a hyperlink to another site, but the other site also has a reversed hyperlink to the targeted site and this reversed hyperlink is compliant with some conditions, eg. the hyperlinked sites and currently evaluated site do not reside at the same domain name space and with different authors. For example, the URL of www.online-service.com is considered the same domain space as the URL of www.online-service.com/dating – and so does not count.
- *Trusted Third Party (TTP):* an authority provides information that the hyperlinked sites are "relevant" to the currently evaluated site. TTP could be the bureau of dating service, which has a registered online dating service listing the URLs of www.find-a-partner.com and www.online-dating.net. This indicates the URL www.find-a-partner.com is related to online dating services. Therefore it is "relevant" to the currently evaluated Web site of www.online-dating.net.
- *Semantic analysis to determine "relevance"*: a way to identify synonyms between hyperlinked sites (ie. the targeted site and a site that is hyperlinked from the targeted site).
- *Web content analysis*: based on matching sub-set of trust attributes with the starting page to determine the current page's relevance to the starting page (eg. Primary Service attribute in Category A). Some Z39.50 information retrieval functions may have potential for content analysis by retrieving hyperlinked Web information from a trust-metadata-base server of TTP (ie. Trust Third Party), which stores the results of recent analysis.
- *A pre-defined set of "relevant-services":* predefined "relevant-services" in the metadata of the starting page flags all relevant services, eg. dating service including restaurant, hotel and travel hyperlinked sites. An industry classification system could be utilised for relevance assessment.
- *Metadata information*: for each classified hyperlinked site (eg. Cat-A external link in W3TM), the "relevance" could be flagged in the Relevance metadata, eg. Relevance = Yes. Then each flagged site will be evaluated and its the total trust value will be accounted for. Any irrelevant hyperlinked sites may or may not attract negative results depending on the selected algorithm.

By matching "relevance attributes" between the targeted Web site and the hyperlinked Web site, a relevance assessment could be carried out as follows:

- Follow each identified external link of the targeted site (eg. Cat-A external link of Category A of W3TM)
- Compare "primary services" attributes between the targeted and hyperlinked sites and ensure both domain names are unique
- If the hyperlinked site's primary service attribute (eg. hotel) is a subset of the targeted site's primary services (eg. dating service, restaurant and hotel), then this hyperlinked site is tagged as "relevant" and is recruited to the relevance-tree. The number of elements in the intersection of the two sites' attributes divided by hyperlinked site's total number of attributes in Primary Services. For example, if the hyperlinked site's primary service attribute has 5 online services (ie. dating, hotel, restaurant, gambling and

entertainment) and the targeted site's primary service attribute has 3 services (dating, hotel restaurant), the common/shared attributes are 3 services. The relevance value could be calculated as 3/5 = 0.6. That is, the R has "relevance-value" of 60%.

- If the relevance-value is greater than or equal to 50%, then the hyperlinked site will be recruited to the relevance-tree.

There are some attributes in categories A (eg. Location, Source, Publisher, company legal registration number), which must be different when assessing "relevance" between two pages. The process of weighting or scoring "relevance" on each referral page may then be viable. R must be between 0 and 1.

6. Subordinate Assessment

S is a numeric value of "subordinate assessment". A targeted page often has hyperlinked pages (sites). These hyperlinked sites could be named as "children" nodes of the parent. A child node is said to be a "subordinate node" of its parent node. Subordinate assessment is trust assessment of hyperlinked child nodes. The result of the assessment is denoted as S. A web page may have a number of child nodes, which also have their own child nodes. The "parent" can have "child" and "grandchild" nodes. The structure of the family among parent, children and grandchildren could be denoted as a graph structure. This graph then is pruned to a tree structure.

The value of S is calculated based on the total trust value TT (see Section 7) of child node and the associated relevance value of the child node (R), and weighted by the total number of children.

The following is an example formula for S. In general case, S = the sum of the combination of the total trust value of children (TT_child) and the relevance values (R_child) of direct-subordinate nodes; that is,

$$S = \sum(TT\_child \times R\_child) / (no.\ children)$$

That means the fewer children, the better the S value. For example, a parent node has one child node. The total trust value of the child node is 0.7 and the R value for the child node is 0.5. The S value of the parent node:

$$S = (0.7 \times 0.5)/1 = 0.35$$

In general, the S value will take total trust value contributions from immediate subordinate nodes and associated R values. The S value must be between 0 and 1.

7. Total Trust Value

TT is the total trust value of each page in the relevance tree. The top node TT is based on TT of each page. TT combines values of P (Section 3), Q (Section 4) and S (Section 6) of the targeted site and associated subordinate nodes in the relevance-tree and normalising the result. In other words, the value of TT is not only based on the standalone page's trust assessment, but also takes account of the "subordinate assessment" of all hyperlinked pages. One special case is the overall trust value of the top node, ie. the targeted site where trust evaluation is required. It is also known as a root node of a relevance-tree in the trust evaluation process.

The value of TT can be found by recursion. TT is a site-based evaluation on the trust value of each hyperlinked site. In other words, collect the trust metadata of all categories for each site and calculate the three trust categories: weight and assign a score to each category, and combine all values to form the total trust value of the currently evaluated page. The following is an example formula [1]:

$$TT = (P+Q+S)/3$$

Different formulae may result in different TT values, but TT must be between 0 and 1.

There are a number of possible formulae, which can be developed based on different theories to calculate the overall trust value of a page (TT), and combine the values P, Q, S of subordinate nodes. It also includes initialisation, weighting and combining of Trust Attributes. For example, the following illustrates options for initialising trust values for 16 trust attributes in Category A:

[1] See www.cs.adfa.edu.au/~yany97/IC2002 for detailed examples.

a. Total number of present attributes of a page is divided by the total number of benchmarked attributes; or
b. Total-Category-Value (95%) is divided by the number of trust attributes. This will give each trust attribute a non-discriminatory equal value; or
c. Divide 16 trust attributes into 3 sub-categories, such as critical, important and trivial. Each sub-category then has been assigned a portion of the total trust value for Category A (ie. 80%); or
d. 16 trust attributes are given an individual initial value according to the customer's assessment criteria.

8. General Issues

Once the assessment process is finished, the trust metadata-base is updated and consumers will be informed. There are a number of ways to present and store the final result of trust assessments, including numeric format, text format, table, diagram and the trust-metadata-base.

9. Future Work

The proposed W3 Trust Model provides a mechanism for the evaluation of trust and transitivity of trust through carefully constructing a trust metadata tree using online service "relevance" assessments, verifying certificate(s) and logically combining the calculated values. There are a number of areas in which the W3 Trust Model will be further developed, including:

- Developing further options, such as a "zero-trust" model and "maximum-trust" model to cater for different user requirements.
- Continue refining the set of trust attributes of the W3 trust model.
- Carrying out a trust evaluation on a larger sample of real online services.
- Generating general guidelines and standards, based on further case studies.

The W3 Trust Model depends on online service providers' Web contents being compliant with a metadata standard. Given wide use of XML in eCommerce environment, the potential benefits of using XML and RDF may be explored for standardising trust metadata.

10. Summary

Recently, user confidence has become a major concern for both providers and consumers of eCommerce. This paper shows a new way to assess the trustworthiness of eCommerce contents and discussed some associated design choices and techniques. Some examples illustrate how to build high trust value Web contents.

The W3 Trust Model provides a way for both online service providers and consumers to communicate using the language of "trust and transitivity of trust" to establish a trust relationship over the Internet.

References

1 Y. Yang, L. Brown, J. Newmarch and E. Lewis, "eCommerce Trust via the Proposed W3 Trust Model", the PACCS01Conference Proceedings, p9-14, July 2001, Australia.

2 Y. Yang, L. Brown, J. Newmarch and E. Lewis, "*A Trusted W3 Model: Transitivity of Trust in a Heterogeneous Web Environment*", the Fifth Australian World Wide Web Conference Proceedings, p59-73, 18-20 April 1999.

3 Y. Yang, L. Brown, J. Newmarch and E. Lewis, "*Trust Metadata: Enabling Trust and a Counterweight to Risks of E-Commerce*", Asia Pacific World Wide Web Conference Proceeding, p197-203, January 2000.

4 Y. Yang, L. Brown, J. Newmarch, "*Token of Trust: Different Certificates for Different Trust Models*", UniForm'99 New Zealand Conference Proceedings, p29-44, 13-17 April 1999.

5 Y. Yang, L. Brown, and J. Newmarch, "*Trust Issues in Public Key Certificates*", AUUG'98 Conference Proceedings, p77-93, 14-18 September 1998.

6 Y. H. Li, "Toward a Qualitative Search Engine", page 24 - 29, *IEEE Internet Computing*, July/August 1998.

7 S. Lawrence and C. Lee Giles, "Context and Page Analysis for Improved Web Search", page 38 - 46, *IEEE Internet Computing*, July/August 1998.

8 M. R. Henzinger, "Hyperlink Analysis for the Web", page 45-50, *IEEE Internet Computing*, January/February 2001.