A Framework for Web Services Trust

Marijke Coetzee and Jan Eloff

Information and Computer Security Architectures (ICSA) Research Group
Department of Computer Science, University of Pretoria, Pretoria, South Africa
marijke@acm.org, eloff@cs.up.ac.za

Abstract. Today, organisations that seek a competitive advantage are adopting virtual infrastructures that share and manage computing resources. The trend is toward implementing collaborating applications supported by web services technology. In order to enable secure interoperation between participants of these environments, trust is an important requirement to address. Current solutions to trust between web components are limited, as they are usually established via cryptographic mechanisms, in the presence of trusted third parties. To accommodate the dynamic and fluid nature of web services environments, a framework for trust assessment and computation is presented. The trust framework is characterised by information and reasoning. It has mechanisms that allow web services entities to manage trust autonomously, by activating a trust level and trust types by means of a rule-based fuzzy cognitive map.

1 Introduction

With the globalisation of the world economy, more and more organisations are realising the need to move to open standards in order to collaborate with business partners. Web Services technology represents a response to the need for a flexible and efficient business collaboration environment. It provides a technical infrastructure to ensure that applications from different organisations can interoperate. Application-to-application interactions automatically perform operations that previously required human interventions, such as searching and buying goods at a pre-determined price, coordinating flight reservations and streamlining invoicing and shipping processes.

Web services are Extensible Markup Language (XML) applications mapped to programs, objects, databases or comprehensive business functions [21]. Web services standards define the format of message that are exchanged, and specify the interface to which the message is sent. The web services architecture is based upon the interactions between three roles [10]: a web services provider that hosts a web service and its operations, a web services broker that makes web services publicly accessible, and a web services requestor that integrates web services operations with its application environment.

The decision to allow cross-domain application integration is critically dependent on whether a business partner can be trusted. In order to establish trust between web services, the Web Services Trust Language or WS-Trust [12] was published. WS-Trust relies on mechanisms such as cryptography, trusted third parties and key

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

management schemes. The resulting trust that is established is of a limited nature, as it does not take into account evidence and previous experiences. Trust management solutions [4, 23] enable cross-domain movement of entities, represented by credentials. The required trust relationships are not easy to establish as they may have to be negotiated, are complex and time-consuming to implement, and are manually configured by administrators.

To address trust requirements for cross-domain application integration, this paper presents a framework for web services trust. The framework gives a web service the ability to determine the trustworthiness of others at execution time, instead of determining such trustworthiness manually or by means of cryptographic PKI frameworks. The framework makes explicit the role of security mechanisms and controls in trust assessment, and identifies additional elements such as competence, over which trust can be formed.

The remainder of this paper is structured as follows: Section 2 gives an example. Section 3 presents a brief background to characteristics of social trust. Section 4 describes these characteristics as they may be applied to web services, and introduces a definition for trust management. Section 5 describes the framework for web services trust. The framework is characterised by automated assessment of information and trust inference. A rule-based Fuzzy Cognitive Map is used to infer a trust level. Section 6 describes a prototype implementation. Section 7 concludes the paper.

2 Motivating example

This example considers eBooks, a web services provider that provides a retail service to sell academic books, and eLoans, a web services requestor. eLoans provides study loans to students. To more effectively manage a student loan, eLoans enables students to purchase books by integrating operations of eBooks at its portal. When eBooks interacts with eLoans, it exposes itself to risk.

When establishing new business relationships with web services requestors, eBooks needs to determine their trustworthiness. A number of checks can be made such as the verification of the identity of eLoans, the country that eLoans is located in, as this may ensure legal protection in the face of misconduct, the credit record of eLoans, contracts and agreements that are in place to provide protection, the existence of insurance against loss, and encryption algorithms used when sensitive information is sent across a network. eBooks has little means to determine the trustworthiness of eLoans other than with time-consuming and expensive processes that quickly become outdated.

To be able to support the instant application integration provided by web services technology, mechanisms are required to dynamically assess the trustworthiness of eLoans. In order to address an automated approach to trust assessment, the next section introduces characteristics of trust to be considered in the framework for web services trust.

3 Trust

Trust between web services requires characteristics of human and organisational behaviour, as decisions need to be made in unfamiliar environments when complete information is not available. From a large body of work on trust [2, 3, 8, 13, 15, 19, 20, 22], the following characteristics of trust are highlighted for the purposes of this research:

1. Trust is used to reduce complexity when decisions are made. In work by Luhman [19], trust is seen as a mechanism used to perceive the complexity of future interactions that may lead to unfavourable outcomes. A trustor has no other choice, than to make a decision to trust, based on limited information known about the other party.

2. Trust is formed from different types of trust. The decomposition of trust is reported in literature. Marsh [20] identifies types over which trust is formed such as competence. Chervany and McKnight [8] defined a high-level typology of trust that identifies the situational decision to trust, dispositional trust, trusting beliefs and system trust. Castelfranchi and Falcone [7] identify honesty and competence as some of their belief components. A model of inter-organisational trust identifies competence, predicatability and goodwill as components of trust between organisations [22].

3. The basis of trust is intuitive reasoning over information. Humans continually assess each other as they collect information through experiences, observations, and recommendations from others [2]. Assumptions are soon made in relationships such as: "it is very likely that Sue is trustworthy". It is not possible for humans to exactly determine Sue's trustworthiness by stating "the probability that Sue is trustworthy is 8". If, because of previous experiences, the general trusting disposition of Jill is to be very distrustful, her trust in the system and in others is lowered.

Trust for eBooks is next investigated, to determine its synergy with mentioned characteristics of human trust.

4 Trust for eBooks

Research on trust formation between applications has had its origins in trust management systems [4, 23]. Trust management [4] makes use of mechanisms such as identities, certificates, signatures and keys to establish trust relationships across domains. Grandison [16] later extended the definition of trust management to: "*the activity of collecting, encoding, analysing and presenting evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships for Internet applications.*" Evidence could include credentials such as certificates for proof of identity or qualifications, risk assessments, usage experience or recommendations. This definition highlights the fact that trust is not only formed over the verification of a digital identity, but also over other categories of information. A drawback of this work is that initial trust values are not computed, but are assigned by an administrator after information and evidence is processed.

In order to enable eBooks to determine the trustworthiness of its web services requestors dynamically, this research aims to extend the definition of trust management to an automated process of trust assessment that includes above-mentioned characteristics of trust as follows:

1. Trust is used to reduce complexity when decisions are made. eBooks makes a decision to trust eLoans, after an evaluation of possibly limited information it has on characteristics of eLoans.

2. Trust is formed from different types of trust. Inspired by the way humans trust, this research maintains that trust between eBooks and eLoans can be formed by three types of trust as follows:

- An assessment of the properties of the *internal environment* of eBooks to establish its self-confidence and its general disposition to its web services requestors.
- An assessment of the properties of the *external environment* or institution within which the trust relation between eBooks and eLoans exists. This increases trust to reflect moderate levels.
- An assessment of the properties of eLoans. Trust evolves and can grow over time to a high level that reflects goodwill.

3. The basis of trust is intuitive reasoning over information. It is not possible to directly portray the intuitive manner in which humans trust. eBooks can exhibit a form of intuitiveness if it can make inferences from incomplete information and can react in unfamiliar situations. This can be achieved if trust information can be identified for the three mentioned trust types. For eBooks, an intuitive trust decision is replaced with a formal process of trust assessment and mathematical reasoning. Trust concepts are numerically formed from information that is arranged together due to similarity. This enables eBooks to follow humanistic reasoning as trust concepts are defined to be fuzzy of nature. eBooks can include tolerance for imprecision, uncertainty and partial truth in its reasoning, similar to the way that humans do.

Based on the above characteristics, the following definition for trust management and of a trust concept is proposed:

Definition - Trust management: *The automated assessment of information and evidence, relating to the properties of the internal environment, the properties of the external environment, and the properties of the other party, with the purpose of establishing trust concepts from which a trust level can be inferred.*

Definition – Trust concept: *A trust concept is a fuzzified category of information or evidence that is populated with a value between 0 and 1.*

5. Framework for web services trust

The framework for web services trust is characterised by a phased approach where trust evolves over time. The automation of trust assessment and formation is supported by the web services architecture as follows:

- *Publish trust information:* Web services providers and requestors needs to inform others how it will behave in order to establish a trust relationship with them, and what it may expect from them.

- *Discover trust information:* Information is gathered by locating and inspecting XML policies, references, and certificates.
- *Trust formation:* XML policies and other information are analysed and evaluated. The result of this phase is a basic level of trust.
- *Trust evolution:* Web services monitor all further SOAP [5] interactions in order to evaluate the trust held towards others. If all transactions are processed smoothly, trust evolves so that future interactions may be granted access to more sensitive resources or risky transactions.

Common sources of information that can be used to form trust are: metadata such as WS-Policy [6] or WSLA (Web Service Level Agreements) [11] documents that is required by complex web services; references and recommendations that are formatted in XML and added to SOAP headers; and experiences that can be recorded by inspecting SOAP messages. The gathering of trust information has been described in a preceding paper by the authors [9].

Fifteen trust concepts are identified for trust formation in the next section, of which some are only named, and others are discussed. Trust concepts such as compliance to agreements, level of vulnerabilities, implemented security mechanisms and predictability represent a realistic view of a web services requestor such as eLoans, and the stability of the environment in which web services operations of eBooks are to be used. Trust concepts embody the beliefs of eBooks to provide a basis over which trust can be inferred. The strength of trust is thus a function of the assessment of information [7].

Trust concepts are interrelated, with feedback links that propagate influences to trust types. Axelrod's work on Cognitive Maps introduced a way to represent such processes [1]. When information is assessed to form trust concepts, numerical data is uncertain, and the formulation of a mathematical model is difficult. Efforts to address this problem should rather rely on natural language statement in the absence of formal models. Fuzzy Cognitive Maps (FCM), as introduced by Kosko [18] is used by this research to address the trust assessment process. This research is inspired by the work of Castelfranchi and Falcone [7], that have shown how humanistic forms of trust can intuitively be mimicked by a FCM. This paper extends their work to application-to-application interactions. The next section describes the approach to trust calculation.

5.1 A proposal for web services trust calculation

In order to enable a web service to form trust relationships with others, a trust manager is proposed. The trust manager, shown in Figure 1, is accommodated in the web services architecture, before any web services interaction takes place. The trust manager is knowledgeable about the requirements of the web service, the standards that are used and the threshold of trust that is required. When requests are sent to a web service, accompanied by references and recommendations, its trust manager will intercept the request in order to verify the validity of information with independent third parties. The trust manager records experiences by inspecting SOAP messages. It also mediates all trust-related interactions with partners and strangers, while it intelligently processes all information that it sources, or that is presented to it.

A FCM, shown in Figure 1, is associated with each web services entity such as eLoans. A web services entity infers a trust level for others according to the structure of the FCM. The FCM enables a web services entity to make intuitive decisions based on observations and experiences. Nodes of a Fuzzy Cognitive Map represent trust concepts that are used to describe main behavioural characteristics of the system. An Interface component intercepts SOAP messages, applies rules to analyse and categorise information, and stores information in a database. The Trust Inference component populates nodes of the FCM with values in the fuzzy interval range [0, 1] after information is fuzzified. Finally, a trust level is inferred. Trust levels are defined as the set {*ignorance, low, moderate, good, high*}, where *ignorance* $\subseteq$ *low* $\subseteq$ *moderate* $\subseteq$ *good* $\subseteq$ *high.*

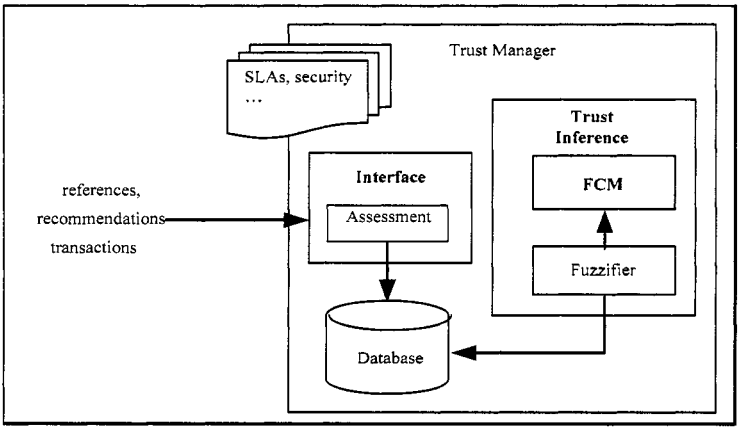

Fig. 1. Web services architecture for trust.

5.2 Trust inference

Fuzzy Cognitive Maps [17] are dynamical systems that relate fuzzy sets and rules. They are fuzzy graph structures that consist of nodes and weighted arcs, which store information. A Fuzzy Cognitive Map can represent the trust-forming process of eBooks in a symbolic manner, similar to the way in which humans cognitively manipulate trust concepts. A Fuzzy Cognitive Map consisting of n concepts is represented by a $1 \times n$ state vector A, which gathers the values of the n concepts; and by an $n \times n$ edge matrix E, with elements e_{ij}. The activation level A_i, for each concept C_i, is calculated by the following rule [18].

$$A_i = f\left(\sum_{j=1}^{n} A_j \, e_{ij}\right)$$

The value of e_{ij} indicates how strongly concept C_i influences C_j. A_i represents the level of activation of a node. A discrete time simulation is performed by iteratively applying a summation and threshold process to state vector A. A_i is the activation

level of concept C_i at time t+1 and A_j is the activation of concept C_j at time t. f is a threshold function that transforms the summation into the interval [0,1]. Next, the FCM of eBooks is described.

5.3 eBooks FCM

The design of the FCM for web services trust is shown in Figure 2. It depicts 4 labeled nodes that represent the three trust types as described below. The remaining 15 nodes represent trust concepts that are populated with fuzzy values. To commence with the discussion on the design of the FCM, the three types of trust and their interrelationships are first discussed. Trust concepts are discussed in next paragraphs.

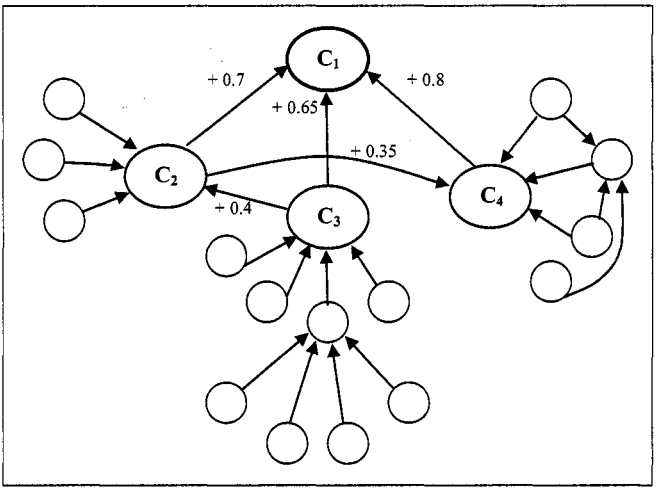

Fig. 2. FCM for trust between eBooks and eLoans.

The concepts representing each node are: $\mathbf{C_1}$ - the trust level that eBooks infers for eLoans, $\mathbf{C_2}$ – the trust in the internal environment of eBooks, $\mathbf{C_3}$ – the trust in the external environment between eBooks and eLoans, and $\mathbf{C_4}$ –the trust that eBooks has in eLoans.

The FCM models the interactions between the three types of trust that form the level of trust that eBooks holds towards eLoans. Input from experts is used to determine causal influences on trust [18]. Each arc is drawn and weighted through intuition and may be modified through experimentation. Causal relationships between concepts are represented by signed and weighted arcs. The arcs of the graph represent the impact that one concept has on another and vary in the interval [-1, +1]. For instance, a value +0.8 for the trust in eLoans (C_4) increase the trust (C_1) by 80%.

- The trust in the internal environment of eBooks (C_2) and the trust in the external environment between eBooks and eLoans (C_3) have a moderate to strong influence on trust as their weights are set to +.7 and +.65 respectively.

- The trust that eBooks has in eLoans (C_4) has a strong influence on trust, as the weight is set to +0.8.
- The trust in the internal environment of eBooks (C_2) has a causal effect on the trust that eBooks has in eLoans (C_4). If eBooks is very sure about the risk of an endeavour and has expertise in dealing with that risk, eBooks can increase its belief in eLoans to reflect its self-confidence.
- The trust in the external environment that exists between eBooks and eLoans (C_3) has a causal effect on the trust in the internal environment of eBooks (C_2). If eBooks is transacting with eLoans in a familiar environment, eBooks is bound to feel very sure of itself, even though it may have vulnerabilities in its environment to consider.

The activation of a trust level (C_1) by trust concepts is implemented by a fuzzy rule. Fuzzy rules map input concepts to an output concept [14]. For this discussion, it is assumed that eBooks requires a high level of trust with eLoans. This is implemented with the following rule in the FCM:

If *the trust in the internal environment* is **sufficient** and
the trust in the external environment is **good** and
the trust in eLoans is **high**
then
the trust level is **high**

The fuzzy rule specifies that all trust concepts must be at a high level for the trust in eLoans to be "high". In order to activate "high" trust, thresholds are set to activate trust concepts. Trust assessment and fuzzification of information sources qualify trust concepts to be at a "high" level. If so, the value of a trust assessment category is set to 1 (otherwise 0). For instance, if information gathered and processed increments the trust assessment of the external environment (C_3) to more than 0.7, it is within the "good" range, and is activated to 1 in order to influence the trust level. In a similar manner, if the trust assessment of requestor Y (C_4) is more than 0.8 and the trust assessment of the internal environment (C_2) is more than 0.75, they are in the "high" range, and are activated to 1. These activation thresholds are defined intuitively.

To activate a trust level (C_1), an activation threshold is set for each trust level. This threshold specifies the minimum strength to which the incoming relationship degrees must be aggregated in order to achieve "high" trust. Trust is "high" if all trust concepts are activated as they become "high". If a web service requires other levels of trust such as "low" or "moderate", thresholds for trust concepts trust types are implemented accordingly. The population of nodes representing the trust types of the FCM is next given.

5.4 Population of trust concepts

The focus of this research is to aim towards an automated process of trust assessment and inference. As the trust in the other party ($\mathbf{C_4}$) is most representative of this aim, it is discussed in the next paragraph. Trust in the internal environment ($\mathbf{C_2}$) and trust in the external environment ($\mathbf{C_3}$) are partly populated by administrator intervention and their automation is the focus of future research. Trust concepts over which they are inferred are briefly described as background to the discussion that follows.

Trust in the internal environment ($\mathbf{C_2}$) is populated after risk assessments have been conducted. Three nodes, show in Figure 3, represent the vulnerabilities in the systems of eBooks, the confidence of eBooks, and the complexity of the systems of eBooks. Trust in the external environment ($\mathbf{C_3}$) is formed by nodes representing legislation that may exist, assurances, compliance, and security mechanisms that are inferred from identity mechanisms used, supported integrity algorithms, supported confidentiality algorithms, and adherence to best practice. These two trust types form a basic level of trust based on risk evaluations, security mechanisms and guarantees, over which trust in eLoans can evolve.

The discussion now focuses on the third trust type, the trust in the other party, eLoans ($\mathbf{C_4}$). For the purpose of activating trust ($\mathbf{C_1}$) with the fuzzy rule, it is assumed that the trust in the internal environment is *sufficient*, and the trust in the external environment is *good*. For trust in eLoans to be *high*, the trust in the properties of eLoans needs to be *high*.

5.4.1 Trust in eLoans

As eBooks interacts with eLoans, it gains information about characteristics of eLoans, organised according to its compliance to agreements, competence and predictability. Over time, the establishment of these characteristics leads to a measure of goodwill. The trust eLoans ($\mathbf{C_4}$) is inferred from related trust concepts as depicted in Figure 3. The concepts representing each node are: $\mathbf{C_{16}}$ – the compliance of eLoans to agreements, $\mathbf{C_{17}}$ – the competence of eLoans, $\mathbf{C_{18}}$ – the predictability of eLoans and $\mathbf{C_{19}}$ – the goodwill developed towards eLoans. A high-level description of the population of each of node with a fuzzy value in the range [0,1] is now given.

C_{16} – eLoans compliance to agreements

Compliance to agreements is the belief that eLoans is honest in its interactions with eBooks. To ensure quality of service, a web services requestor and provider jointly defines a machine-readable service level agreement (SLA) as a part of a service contract that can be monitored by one or both parties. Such agreements are defined in XML-based policies with either WS-Policy or WSLA, and are monitored. The compliance of web services requestors to agreements can be determined by inspecting a large variety of parameters. For this discussion, eBooks monitors the following two parameters:

- The SLA may state that no more than 10 transactions are allowed per minute. If this restriction is exceeded, a record is written to a database to indicate the level transgression by using a factor between 1 and 10, where 10 represents the worst case.
- Security requirements may be stated in WS-policy documents. If eLoans does not adhere to these requirements, it can be recorded to a database as an improper event. Records are written to the database according to a predefined set of rules. Records are aggregated to a value between 0 and 1 to indicate the level of compliance. For instance, if a value of .45 is derived, the level of compliance to agreements is *not sufficient*. A value of .8 means that the level of compliance to agreements is *good*. The causal relationship reflects the fact that if eLoans complies with agreements, the trust in it increases by .5.

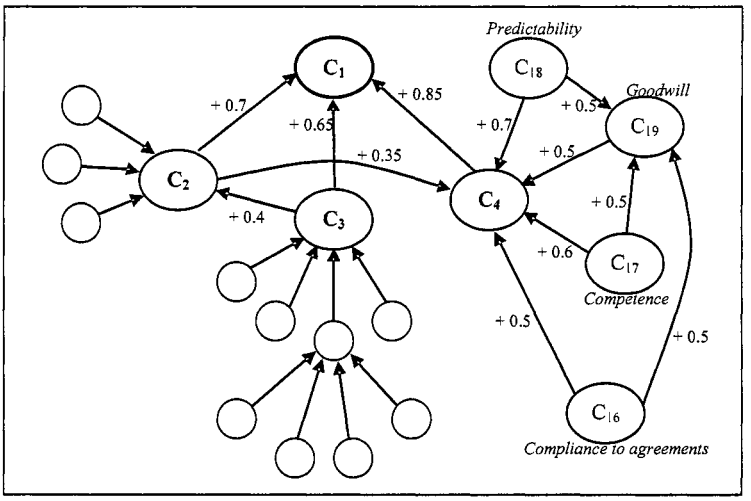

Fig. 3. Activation of trust in eLoans.

C_{17} – The competence of eLoans
Competence is the belief that eLoans has the ability or necessary skills to perform a task. The competence of eLoans can be determined by evaluating recommendations and references that are submitted. Certificates state competence levels such as credit ratings, audit information, endorsements, ISO 9000 certification, privacy seals, or Better Business Bureau statements. Recommendations from other entities are also used to determine competence. Recommendations are only accepted from entities that are identified by a public key. The trust in the public key, determined by trust computation where possible, determines the weight assigned to a recommendation.

Recommendations, references and other statements are evaluated and a value between 0 and 1 is derived to populate node C_{17}. For instance, if a value of .3 is derived, the competence of eLoans is *low*. A value of .8 means that the level of competence is *high*. The causal relationship reflects the fact that if eLoans is competent, the trust in it increases by .6.

C_{18} – The predictability of eLoans
Predictability is the belief that the actions of eLoans is consistent, so that a forecast can be made about how eLoans will behave in a given situation. This can be achieved by inspecting SOAP messages that are sent and received, and by recording for instance, the number of messages, the number of messages in error, the value of transactions, date of transaction fulfillments, and the validity of message details. The focus of this monitoring is to determine a score for each interaction from when a transaction is initiated, until it is fulfilled. If, for instance, an invalid credit card is submitted, the level of transgression is recorded by taking into account the value of the transaction.

The score for each interaction is evaluated and a value between 0 and 1 is derived to populate node C_{18}. For instance, if a value between .5 and .65 is derived, the predictability of eLoans is *moderate*. A value of .8 means that the level of predictability is *high*. The causal relationship reflects the fact that if eLoans is predictable, the trust in it increases by .7.

C_{19} – The goodwill held towards eLoans
Goodwill is the belief that eLoans cares about the welfare of eBooks. It is not established by an assessment of information, but is rather established over time as eBooks realises the benefits gained from increased cooperation with eLoans. Thresholds are set for compliance to agreements, competence and predictability to computationally infer goodwill. The activation of the level of goodwill (C_{19}) by related trust concepts is implemented by a fuzzy rule. In order to have a high level of goodwill towards eLoans, the following rule is used:

If *the compliance of eLoans to agreements is* **good** and
the competence of eLoans is **high** and
the predictability of eLoans is **high**
then
the goodwill towards eLoans is **high**

Causal relationships reflect the fact that as eLoans complies with agreements, is found to be competent, and predictable, goodwill increases in each case by .5.

6 Prototype

A prototype of limited scope was implemented to illustrate the viability of the trust assessment framework. Trust in the internal and external environment currently populated by administrator intervention, and its automation is the focus of future research. The prototype was developed in the .NET platform. It consists out of the Interface component, a database, and the Trust Inference component.

The interface component is implemented as a SOAP extension, and intercepts all SOAP requests. Requests are inspected to determine the nature of the information that it carries. Information is categorised according to predefined rules, and stored in a database. Information is time-stamped to ensure that out-dated information can be discarded. The database consists out of a variety of tables where different types of information are stored. All tables relate to the identity of a web service requestor.

Next, the trust inference component interrogates tables from the database, and fuzzifies information to populate nodes of the Fuzzy Cognitive Map with values between 0 and 1. The FCM is finally invoked. It infers a trust level over all trust types and trust components. Values for trust types and final trust are time-stamped and stored in a table in the database for future references by for instance, an authorisation component.

7 Conclusion

Experimentation shows that the FCM performs well. A gradual increase in trust is evident as trust concepts are populated. Small changes in trust concepts do not affect the level of trust. The approach to trust is highly intuitive and is based on incomplete information. The FCM enables eBooks to identity reliable business partners with whom it can foster stronger and more meaningful relationships, as eLoans can only achieve a high level of trust if it consistently behaves well. An important contribution made by this research is that trust is composed from different trust types. In some situations, it may be important to interact with parties with whom no familiarity exists, but in the knowledge that the trust in the environment is high.

Even though trust is built by exchanging digital credentials, trust is not built iteratively as in automated trust negotiation (ATN) systems [24]. A trust level is calculated, that reflects a history of interactions and other characteristics of a web services entity and its environment. In a similar vein to this work, trust is computed in the SECURE project [25] over information and evidence. In SECURE, the structure of information is not made explicit, and the approach to trust calculation is not intuitive.

This research is a first step towards an automated trust formation process for web services. It is unique in that trust types and trust concepts are identified for web services environments that are practical to implement. The structure of the FCM can be considered as the main contribution of the paper. It is illustrated that much of the required information is available in machine-readable format, and can thus automatically be gathered and assessed. The causal relationships and fuzzy rules are still the focus of much experimentation. It is important to note that an individualised FCM can reflect the personal considerations of a web service, such as confidence, steadiness, or knowledge of vulnerabilities, by the manner in which causal weights are assigned.

n important focus of further research is identifying problems with the input and output of the FCM, and the assigning of the weights of the causal links. This may be helped by computational training methods, but there is no certainty that the single best set of causal links will be found.

Acknowledgement

The financial assistance of the Department of Labour (DoL), the National Research Foundation (NRF) in South Africa under Grant Number 2054024, Telkom and the IST through THRIP towards the current research is hereby acknowledged.

References

1. Axelrod, R., Framework for a General Theory of Cognition. Berkeley: Institute of International Studies, (1972).

2. Abdul-Rahman A., A framework for desentralised trust reasoning, PHD thesis. Department of Computer Science, University of London, (2004).
3. Barber B., Logic and Limits of Trust. New Jersey: Rutgers University Press, (1983).
4. Blaze M., Feigenbaum J., Ioannidis J., & Keromytis A., "The KeyNote Trust-management System, version 2," IETF, RFC 2704, September, (1999).
5. Box D., Ehnebuske D., Kakivaya G., Layman A., Mendelsohn N., Nielsen H.F, Thatte S. & Winer D., (2000), Simple Object Access Protocol (SOAP) 1.1, http://www.w3.org/TR/SOAP/, May (2000).
6. Box D., Web Services Policy Framework (WS-Policy), http://www.ibm.com/developerworks/library/ws-policy/index.html, (2003).
7. Castelfranchi C, Falcone R., Pezzulo G., A Fuzzy Approach to a Belief-Based Trust Computation., in Trust, reputation and security theory and practice, Bologna, Italy, July,Lecture notes in Computer Science, Vol 2631, (2002).
8. Chervany N.L. & Mgknight D.H., The meanings of trust. Technical Report 94-04, Carlson School of Management, University of Minnesota, (1996).
9. Coetzee M. & Eloff JHP, Autonomous trust for Web Services, INC 2005 (The 5th International Network Conference), 5 – 7 July, Samos, Greece, (2005) Also available at http://csweb.rau.ac.za/staff/marijke/marijke_coetzee.htm.
10. Coyle F.P., XML, Web services and the data revolution, Addison-Wesley, (2002).
11. Dan A., Davis D., Kearney R., King R., Keller A., Kuebler D., Ludwig H., Polan, M. Spreitzer, and Youssef A., Web Services on demand: WSLA-driven Automated M. Management, IBM Systems Journal, Special Issue on Utility Computing, Volume 43, Number 1, pages 136-158, IBM Corporation, March, (2004).
12. Della-Libera G. et al., Web Services Trust Language (WS-Trust), http://www.ibm.com/developerworks/library/ws-trust/index.html, (2003).
13. Deutsch M., Cooperation and Trust: Some theoretical notes, in Nebraska Symposium on Motivation, M.R. Jones (ed.) Nebraska University Press, (1962).
14. Eloff J.H.P. & Smith E., Cognitive fuzzy modeling for enhanced risk assessment in a health care institution, IEEE Intelligent systems and their applications, Vol 14, no 2, pp 2-8, (2000).
15. Gambetta D., Can we trust Trust?, Chapter 13, pp. 213-237. Basil Blackwell. Reprinted in electronic edition from Department of Sociology, University of Oxford (1988).
16. Grandison T.W.A., Trust Management for Internet Applications, PhD Thesis, Imperial College of Science, Technology and Medicine, University of London, Department of Computing, (2003).
17. Kosko B., Fuzzy Cognitive Maps, International Journal of Man-Machine Studies, Vol 24, pp 65-75, (1986).
18. Kosko B., Fuzzy Engineering, Prentice Hall, Upper Saddle River, New Jersey, (1997).
19. Luhman N., Trust and Power. Wiley, (1979).
20. Marsh S., Formalising Trust as a Computational Concept, PhD Thesis, University of Stirling, UK, (1994).
21. Newcomer E. Understanding Web Services, Addison-Wesley, USA. (2002).
22. Ratnasingam P.P., Interorganizational trust in Business to Business e-commerce, PhD thesis, Erasmus University Rotterdam, (2001).
23. Rivest R. & Lampson B., "SDSI - A Simple Distributed Security Infrastructure," October (1996).
24. Winslett M. An Introduction to Trust Negotiation. Nixon & Terzis (eds), In Proceedings of the First International Conference, iTrust Heraklion, Crete, Greece, May 28-30, Springer. (2002).
25. SECURE, Bacon J., Belokosztolszki A., Dimmock N., Eyers D., Moody K., Using Trust and Risk in Role-Based Access Control Policies, Proceedings of Symposium on Access Control Models and Technologies SACMAT04, (2004).