Composite Web Services Security Considerations

Reinhardt van Rooyen
Computer Science Department
University of Cape Town
Cape Town, South Africa
Email: rvanrooy@cs.uct.ac.za

Andrew Hutchison
Computer Science Department
University of Cape Town
Cape Town, South Africa
Email: hutch@cs.uct.ac.za

Abstract— **Web services are modular, self describing software components that can be invoked over a distributed network. A single transaction can be composed of many individual Web services.**

There are many security considerations that have to be taken into account when assessing such a Web service transaction. This paper investigates the security concerns involved in composite Web services and introduces at the relevant security standards and legislation as motivation for a trust assurance protocol. In this paper, we focus on the transaction path elicitation in Web services transactions so that trust may be established in an environment where near-perfect information can be achieved.

I. INTRODUCTION

Web services are becoming a standard way of interacting with business partners and service providers in order to provide business solutions. The advantages of Web services are that they can connect parties regardless of their operating platforms and programming implementations. This means that heterogeneous applications can interconnect and work together on a problem without having to spend too much time configuring the environment to allow parties to communicate effectively. A Web services transaction involves two or more parties that take part in processing a task to achieve a particular goal. Web services can be chained together, each adding its services to the overall transaction until it is completed.

Chains spanning multiple services are generally invisible to the original requestor, who has the impression of a simple request-reply transaction with only one partner. In reality, the business partner could include other service providers and generally has to include partners such as merchant banks and other financial institutions into a business transaction. The original requestor of the service has no say in how external services handle its personal information and in most cases, is not even aware of another service provider's presence in the transaction [1].

The threat of online fraud and misuse of personal or personally identifying information (PII) and the interception of Web services messages by malicious third parties has created a mass of activity to secure Web services. WS-Security[2] has become the leading standards upon which security specifications can be based to become an overall framework in which Web services messages can be secured. This allows a requestor to be confident that communication between itself and the service provider is kept confidential and that the message's integrity is ensured.

Even with the current specifications and standards, the requestor does not have enough control over what a service provider does with personal information once he has received it. Policy languages for Web services which defines what either party may and may not do with the information exist to combat this eventuality, including WS-Policy[3] and the Web services Policy Language (WSPL). In a transaction that is made up of more than one service provider, the client has no knowledge of how the service provider sends their information to another service provider, and cannot influence the decision over which parties the service should interact with. The policy reached between two service providers might not be acceptable to the original requestor, but he has no control over the use of his information in the communication between the two parties. If the original requestor was concerned with the protection of his personal privacy, he might prefer not to engage in the transaction at all if he couldn't be sure of who has access to his personal information, and what they intend to do with the information they do receive [4].

This paper looks at the environment in which Web services can be chained together to form composite chains to successfully complete a Web service transaction. It highlights the relevant standards and outlines the requirements to create transactions in a manner that suits both the Web service requestor and Web service provider such that it falls under the legislation of online transactions and provides motivation for a trust assurance protocol that can be used to control a transaction given these security concerns.

II. BACKGROUND

Web services are poised to become the next generation middleware for distributed computing. It will replace proprietary middleware solutions with a simpler, standards-based system. It achieves simplicity by sending all data between two parties as well formed text messages. Web services make use of the SOAP standard [5] for the purpose of formatting text messages in a structured, standardised format. SOAP is a lightweight communication protocol based on the XML standard. It is beneficial to base Web services on the SOAP standard as it is a transport independent protocol, meaning that a SOAP message can be passed on any existing or future data transport protocol. SOAP enables distributed applications to communicate, regardless of the implementation details of either party.
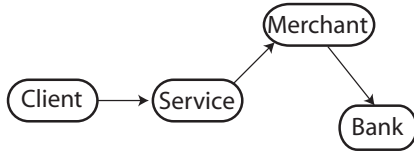
Fig. 1.   Composite Web services chain

Fig. 2.   Web services security stack

The features of the new middleware computing model means that distributed computing systems are now more loosely-coupled than ever before. It has become easier to interconnect computing applications both within a company's internal network as well as external to the network. IBM's definition of Web services states that "Web services are self-contained, modular applications that can be described, published, located, and invoked over a network, generally, the World Wide Web." [6] This positions Web services as external interfaces to applications within a company's internal network. Web services can be described, so that a client, or Web Service consumer, can ascertain whether or not a web service will meet his requirements. The Web service consumer can then locate the service at the network address contained in the description of the Web service and can invoke the service to fulfill his requirements.

The potential of Web services has allowed new business opportunities for companies to expose their internal systems to trusted business partners and also to exploit their own systems as potential revenue streams by exposing their services to unknown parties in ad-hoc business transactions. Because Web services are self contained systems, they can be linked so that many Web services can partake in a single transaction. For example, in *figure 1*, a Web services producer involved in a transaction with the Web services consumer can invoke the services of a Web services enabled credit checking company to see whether the Web services consumer can pay for the right to use the Web Service. The merchant bank can then in turn call the client's bank to confirm payment details or credit information.

All these aspects of Web services makes it easier to intercommunicate between organisations and, unfortunately, introduces a real security concerns in using Web services and allowing others to use your own systems exposed as Web services. Web services are still susceptible to conventional security risks inherent in allowing two parties to communicate and share confidential data, but also new security risks. For example, because Web services messages can travel on existing transport protocols, the most popular protocol on the internet being HTTP at the moment, Web services messages effectively bypass conventional firewalls and intrusion detection systems because they appear as normal website traffic to both of these systems. This makes malicious SOAP messages a threat as they can not easily be detected and dealt with.
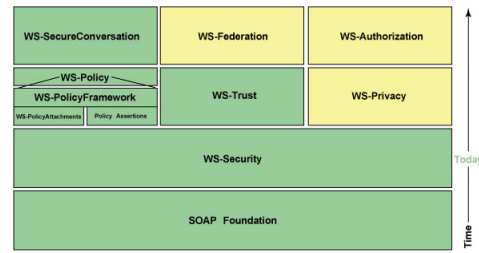
A lot of activity has taken place in attempts to add comprehensive security to SOAP messages. Current transport level security mechanisms such as SSL aren't necessarily sufficient to secure SOAP messages. The reasons for this is listed below:

- SOAP messages may involve multiple parties
- SOAP messages can be sent over any transport protocol

1) Multiple party transactions: SOAP messages can be secured by transport level security if there are only two parties involved and they are directly communicating. In such a case, the Web services provider and the Web service consumer can set up a SSL connection between themselves and send the SOAP message through the encrypted pipe. However, SOAP messages have the capability to be sent to the eventual user of the Web service via one or more intermediaries. These intermediaries could, for example, validate the SOAP message, could add a security token or time-stamp information. If transport level security is used to secure the message between the Web service consumer and web service producer, communication with external services would force the companies to set up another SSL connection between those two parties and it would be impossible to route and modify the message between parties without first decrypting the entire payload and then re-encrypting it at every leg of the transfer.

2) Transport Protocol independence: SOAP was designed to be independent of transport protocols. If Web services security incorporated security mechanisms used in transport level security, it would invalidate the security of Web services if any other transport protocol is used to transport the Web service. Web services security independent of any transport level security is needed to ensure the security of Web services if new transport protocols supersede existing protocols.

A. *Web services security standards*

Many specifications and standards have emerged to provide transport level independent security for Web services. The Web services security framework has now become mature enough to consider using it for distributed applications. *figure two* illustrates the general architecture for Web services security. The standards are based upon previous standards in the stack and extend their capabilities to allow new functionality. There are however, more complicated issues to be resolved before Web services will become synonymous with electronic commerce and electronic transactions. Most companies are using Web services as an interface to existing systems that the companies

use to conduct business in an off-line world. Web services allow these companies to accept transaction requests from the internet. The companies however, treat the transaction request in the same manner in which they process off-line transaction requests. It is here where problems occur between the two paradigms. There are a lot more regulations and legislation concerned with the transfer of electronic information. The regulations try to ensure that the rights of consumers and service providers are respected in any transaction. Off-line transactions represent transactions that are recognised by law and that can be use a countries legal system to resolve disputes if they arise. Personal information regulations describing the collection, storage and dissemination of personally identifiable information (PII) differ between conventional business transactions and electronic transactions. This will be discussed in more detail in the following section.

In the online world, regulations and legislation is still in its infancy, and the problems that lawmakers face are multiplied when transactions span multiple countries, many who do not even have legislation for the protection of online transactions. As an Example, the United States of America has no federal legislation providing for data privacy in electronic communications. Instead, America has several Acts for particular sectors, such as the Financial Modernization Act of 1999, also known as the Gramm-Leach Bliley Act[7], which includes provisions to protect consumers' personal financial information held by financial institutions. Similarly, the Health Insurance Portability and Accountability Act of 1996, known as the HIPAA act, provides requirements for the storage of pesonal information so that the information cannot be shared between institutions without the patient's consent. These sector specific legislative safeguards provide guidance about what is required for general personal privacy protection and self regulatory bodies exist to provide these measures.

Compared to the European union where privacy protection is a legislative concern, electronic transactions between companies that reside in America and the European Union is non-trivial. In fact, the European unions legislation prohibits electronic transactions with member states and countries who do not have acceptable privacy protection laws to protect the members of the European Union. The European Union had to make an exception to allow electronic transactions with America because America is a major trade partner with the European Union.

Agreements between Web services are can be very complicated, and negotiation is required so that all the parties involved in the transaction are satisfied with the conditions under which the Web service will run. Web services specifications

B. Data Privacy Laws

Data privacy has become a paramount concern in electronic transactions. Studies of websites have shown that the number of websites displaying privacy policy information has increased from 14% in 1998 to over 88% in 200 [8]. This has mostly been a self-regulatory step as commercial websites

has addressed the concerns of customers who make use of commercial websites.

The need for legal acknowledgement of electronic transactions has spurred a lot of activity in legislative sectors to recognise electronic data as legal equivalents of paper based transactions. The United Nations Commission of International Trade Law created an electronic commerce (UNCITRAL) model law to describe which aspects of electronic commerce should be enforced by legislative measures [9]. This model law has influenced the creation of legislation in over 25 countries, Including the United States of America, England, France, South Africa ,China and many more. While these laws give credence to the validity of electronic transactions, the laws do not necessarily include concepts of a consumers or client's right to data privacy. The problem of ensuring data privacy protection can be achieved in two different ways. Firstly, there are legislative measures which enshrine a user's right into law, and secondly, there a self-regulatory standards that apply to specific sectors. In particular, America has decided to regulate certain sectors in terms of personal privacy protection. The most recognised American regulations concerning protection of personally identifiable information collected electronically are:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Children's Online Privacy Protection Act of 1998 (COPPA)
- Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act"

All the laws above provide specific laws defining how companies should treat personal information. These laws have caused as much turmoil to the operations of online websites as they have provided benefits. As an example, The number of complaints to hotmail, a web-based email service increased by 1,150% in April and May 2000 after it implemented safeguards listed in COPPA [8]. This example shows that legislation cannot provide a panacea for all privacy concerns, and in fact, under the COPPA act, in some cases the customer had to reveal more information about themselves to prove their age. However, legislation is crucial to the wider adoption of electronic commerce. Until a customer can be given the guarantees that other forms of commerce can, it will never grow into the market it is envisaged to be. A customer must be confident that it can use its countries legal system to resolve disputes.

The European council and member states recognise this fact and the members states are proceeding to roll out legislation derived from the UNCITRAL model law and the European Council's directives on privacy and electronic communications [10]. The directive, known as Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 defines personal information, who holds the rights to personal information and what rights are given to the person who the personal information identifies. This Directive was created for the electronic communications sector and extends the more

general Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [11]. The details of the legislative initiatives are beyond the scope of this paper and are merely illustrating the negotiations necessary before legally binding electronic transactions can take place which will ensure that the users personal information used collected, stored and disseminated according to the law or the wishes of the client.

Legislative laws, such as South Africa's Electronic Communications and Transaction ACT 25 of 2002 [12] define several roles that service providers must fulfill and sets out the requirements of electronically binding contracts, rules for companies selling goods or providing services online and defines what information is considered personally identifiable information (PII) and specifies how companies should handle such information. Legislation like the ECT act gives consumers more right to contest business transaction and unlawful use of their PII. The ECT act of 2002 is derived from the UNCITRAL Model law for electronic commerce. It therefore stands to reason, that Web services based in South Africa should be able to negotiate appropriate terms under which to exchange personal information with other countries that provide similar laws.

Web services must work within these laws and provide users with the confidence that the entire Web services transaction can be logged so that an authoritative body can determine who was involved in a business transaction and what role they played in that particular transaction. The following section introduces the need for a framework in which such an auditing trail can be created.

III. TRANSACTION PATH ELICITATION

This is the first step in creating a policy for a Web service transactions incorporating multiple services. For every Web Services transaction, there must be a finite number of services involved in a certain Web Service transaction. Finding a chain of services involved in a transaction can be done by requesting a list of services from a service provider that that service provider needs to contact in order to complete the transaction. Given the list, each service on the list can then be called to find out which services they will need to use to complete their service. Using this technique, a Web service transaction chain can be mapped recursively. Multiple routes and choices could also be returned by service providers if there are more than one service that can be used to complete a particular part of a service. An example might be a list of certificate authorities. The client will then be able to chose the best transaction path for the transaction based on its own risk assessment of the transaction chains.

Standards groups and Industry partners have created specifications which can be used to elicit the parties involved in the transaction path. In *table 1* a brief list is given.

These specifications all involve coordinating various business processes at different levels. WS-Context[13] provides

TABLE I
LIST OF SPECIFICATIONS DEALING WITH TRANSACTIONS

Specification	Standards Body
WS-Context	OASIS
WS-Coordination	IBM, BEA Systems, Microsoft, Arjuna, Hitachi, IONA
WS-AtomicTransaction	WIBM, BEA Systems, Microsoft, Arjuna, Hitachi, IONA
WS-BusinessActivity	IBM, BEA Systems, Microsoft, Arjuna, Hitachi, IONA
WS-Choreography	W3C

mechanisms for managing information such as security tokens and identifiers that is used in transactions involving multiple parties.

WS-Choreography[14] provides an information model that describes the sequence in which data tokens are passed between two or more participants to achieve a business goal. WS-Choreography also defines the relationship between the data tokens which are passed between parties involved in the transaction.

WS-Coordination[15] is a specification for providing protocols that coordinate transactions across multiple parties. It allows a context to be created in which a transaction can be run and is meant to be extended by other specifications to deliver more concrete transaction coordination. WS-AtomicTransaction and WS-BusinessActivity are both extensions of WS-Coordination and provides rules for business transactions that conform to ACID properties and longer running asynchronous business transactions respectively.

It can be seen from the various groups working on these specifications that there is a lot of interest in composite Web services. However, all these specifications still need a way to determine the trustworthiness of the services that they engage in. These specifications all deal with the functional requirements of the services involved in the transaction. In [16], Van Rooyen and Hutchison outlined a trust assurance protocol and trust determination technique that allows trust and policy requirements to provide the necessary framework so that disparate Web services can engage in complex business transactions with confidence.

Eliciting the entire transaction path and negotiating the privacy policies between all the parties involved in the transaction can range from trivial assertions made to each service provider, or can involve a multiple party negotiation process. However, regardless of how the details of the transaction policy is formed, the initial steps of the framework remain the same. The following sections provide more detail on how a transaction policy can be formed. First the transaction path must be found, the services rated and policies negotiated.

The protection of personal information in distributed transactions involving more than one service provider, coupled with information about each service providers' trustworthiness will create a more secure environment which will spur the creation of services and open up new business revenue streams. It is against this background that the author's a creating a trust

assurance protocol, to determine the dyadic trust that can be determined between the client and a service provider. The measure of trust can be chained together to measure the trust involved in the entire transaction chain. The protocol is an extension of the WS-Policy and WS-Trust specifications and combines contract law with internet commerce legislation, taking into account conflict resolution arbitration and jurisdiction.

IV. CONCLUSION

Electronic communications and transactions require more safeguards and legal restrictions than conventional transactions. With signed electronic documents now being accepted as legally binding documents in more and more countries, precautions are needed to ensure that commercial transactions cannot easily be compromised or falsified. It is vital to ensure that any transaction can be audited and held up to the scrutiny of courts of law. Anonymity services cannot have a place in legally binding transactions, unless the true information can be recovered and revealed if the need arises and they use of anonymising systems do not contravene any legislation that requires a data controller to keep the information on record. It is not the fact that PII has been transferred that electronic transactions requires anonymity services, but rather that a person or company has a legal recourse if his PII is abused.

Composite Web services require both legislature and contractual agreement between the parties involved to allow heterogenous services to interact in a safe and secure manner. This paper highlighted the security concerns in transactions that span multiple parties and acts as a motivation for more advanced trust assurance protocols.

REFERENCES

[1] M. A. Nasir, "Legal issues involved in e-commerce," http://www.acm.org/ubiquity/views/v4i49_nasir.html, February 2004.

[2] A. Nadalin, C. Kaler, P. Hallam-Baker, and R. Monzillo, "Soap message security 1.0 (ws-security 2004)," OASIS, Tech. Rep., 2004.

[3] V. J. Authors, "Web services policy framework (wspolicy)." [Online]. Available: citeseer.ist.psu.edu/703689.html

[4] C. Jensen and C. Potts, "Privacy policies as decision-making tools: an evaluation of online privacy notices," in *CHI '04: Proceedings of the SIGCHI conference on Human factors in computing systems*. New York, NY, USA: ACM Press, 2004, pp. 471–478.

[5] M. Gudgin, M. Hadley, N. Mendelsohn, J.-J. Moreau, and H. F. Nielsen, "Soap version 1.2," W3C, Tech. Rep., 2003.

[6] IBM, "Web services definition," http://xml.coverpages.org/ni2001-02-19-b.html, 2001.

[7] F. T. Commision, "Gramm-leach-bliley bill," November 1999.

[8] R. Hahn, "An assessment of the costs of proposed online privacy legislation," May 2001, aEI-Brookings Joint Center for Regulatory Studies.

[9] United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Commerce," 1996.

[10] European Parliament and Council, "Directive 2002/58/EC of the European Parliament and of the Council," July 2002.

[11] ——, "Directive 95/46/EC of the European Parliament and of the Council," October 1995.

[12] Parliament of the Republic of South Africa, "Electronic Communications and Transactions Act," July 2002.

[13] M. L. E. Newcomer and G. Pavlik, "Web services context specification (ws-context) draft version 0.8," http://www.w3.org/TR/2002/NOTE-wsci-20020808, November 2004.

[14] W3C, "Web services choreography interface (wsci) version 1.0," http://www.w3.org/TR/2002/NOTE-wsci-20020808, August 2002.

[15] M. A. H. I. IBM, BEA Systems, "Web services coordination (ws-coordination) 1.0," August 2005.

[16] R. van Rooyen and A. Hutchison, "Web services transactions assurance," April 2006.