Negotiated Security Policies for E-Services and Web Services

Yee, George; Korba, Larry

Publisher's version / Version de l'éditeur:

Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005), 2005

NRC Publications Archive Record / Notice des Archives des publications du CNRC :
https://nrc-publications.canada.ca/eng/view/object/?id=2236b48f-4999-428a-91ac-ef0809a4fb77
https://publications-cnrc.canada.ca/fra/voir/objet/?id=2236b48f-4999-428a-91ac-ef0809a4fb77

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Negotiated Security Policies for E-Services and Web Services *

Yee, G., and Korba, L.
July 2005

* published in the Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005). Orlando, Florida, USA. July 11-15, 2005. NRC 47449.

Canada

Negotiated Security Policies for E-Services and Web Services[1]

George Yee and Larry Korba
Institute for Information Technology
National Research Council Canada
{George.Yee, Larry.Korba}@nrc-cnrc.gc.ca

Abstract

The growth of the Internet has been accompanied by the growth of e-services (e.g. e-commerce, e-health). This proliferation of e-services and the increasing attacks on them by malicious individuals have highlighted the need for e-service security. The security requirements of an e-service may be specified in an e-service security policy. The provider of the e-service is then responsible for implementing the security measures contained in the policy. However, a service consumer may have security preferences that are not reflected in the provider's e-service security policy (e.g. defense contractors may require higher levels of security). In order for service providers to reach a wider market, a way of customizing a security policy to a particular consumer is needed. We derive the content of an e-service security policy and propose a flexible approach that will allow an e-service provider and consumer to negotiate to an agreed-upon e-service security policy. In addition, we examine how our approach may be implemented in a Web Services environment and briefly describe the design of our security policy negotiation prototype.

1. Introduction

An avalanche of e-services targeting consumers has accompanied the rapid growth of the Internet. E-services are available for banking, shopping, learning, healthcare, and Government Online, to name a few. However, these services are subject to malicious attack in one form or another. This leads to concerns over their security [1].

In order for e-services to be successful, they must be secured from malicious individuals who constantly try to compromise them. An effective and flexible way of managing security for e-services is to make use of security policies. An e-service security policy is a specification of what security measures will be used to protect the e-service from security attacks. A security policy by itself does not guarantee that its stated security measures will be put in place or be complied with. That is an area of policy compliance that is outside the scope of this paper.

An e-service provider makes use of a security policy to specify the security measures that he/she has put or will put in place to protect his/her e-services. However, this security policy may not match up with the security preferences of some would-be consumer of the provider's e-services. For example, suppose the security measure is user authentication by the use of a password. This authentication approach is known to be insecure. A security-sensitive consumer such as, for example, a defense contractor, may wish to add biometric authentication. In such a case, the defense contractor would not be able to make use of the provider's e-service. As another example, suppose the security measure is access control. The provider's security policy may provide access to 5 features of an e-service, whereas a particular consumer may need access to only 3 features. In this case, the consumer may be reluctant to make use of this provider's e-service, especially if the consumer can find another provider that only offers the features needed and at a lower price. One solution to these mismatches of a provider's security policy with a consumer's security preferences is to allow the consumer to negotiate with the provider regarding the security measures that are in the provider's security policy.

The objectives and contributions of this paper are to a) introduce the need for customization of provider security policies on a per consumer basis, b) present an approach for consumer-provider negotiation that accomplishes this customization, including a novel method of providing help during negotiation, and c) describe an effective interface (our prototype) for security policy negotiation. In pursuing these objectives, we derive our version of an e-service security policy but we do not claim that this version is final. Indeed, our proposed content will change over time as new security needs are discovered and previous ones become obsolete.

In the literature, there are many papers related to security policies. Security policies have traditionally been used to specify security requirements for networks and distributed systems [2]. More recently, they have been applied to manage security for distributed multimedia services [3] and for very large, dynamically changing groups of participants in, for example, joint command of armed forces for some time period [4]. In addition, Ventuneac et al [5] describe a policy-based security framework for web-enabled applications, focusing on role-based security policies and mechanisms. They do not mention the need for policy negotiation.

In terms of the literature on security policy negotiation, the available papers largely describe security policy negotiation across Internet domains needed to manage cross domain network security (e.g. [6, 7, 8]), negotiated resource sharing agreements between members of coalitions [9], and security policy mediation between heterogeneous information systems [10] for secure interoperation. We are not aware of any work that deals directly with the negotiation of a security policy between a consumer and a provider of an e-service, as presented here.

It is worthwhile mentioning a related area of negotiation that has a large body of literature: trust negotiation. Trust negotiation is applied to situations where peers need to interact across a network (such as the Internet) and the peers are complete strangers to one another. Trust negotiation is used to establish trust between such peers by iteratively exchanging certified digital credentials. Examples of papers on trust negotiation are [11, 12, 13]. For this work we view trust negotiation as complementary but not needed in most cases of provider-consumer relationship. This is because providers of e-services have ways of making themselves known to consumers (e.g. advertising) and readily conduct business with strangers (with appropriate safeguards).

The remainder of this paper is organized as follows. Section 2 defines e-services and derives requirements for security policies and their negotiation. Section 3 presents our approach for the negotiation of security policies for e-services that satisfies the requirements of Section 2. Section 3 also describes how our approach can be applied to web services. Section 4 gives an overview of our prototype. Finally, Section 5 presents our conclusions and areas for future work.

2. E-Services and requirements for security policies and security policy negotiation

In this section, we begin by defining what we mean by an e-service. We then describe security policy requirements and security policy negotiation requirements.

2.1. E-Services

An e-service for the purposes of this paper is characterized by the following attributes:

- The service is performed by application software (service software) that is owned by a provider (usually a company); the service is accessible across the Internet.
- The provider's service software can make use of the service software of other providers in order to perform its service; in this case, the provider is also a consumer.
- A provider can have more than one e-service.
- The provider has a security policy that specifies what security measures he will use to secure his service(s).
- The provider also has a privacy policy that spells out what consumer private information is needed to perform the service and how the private information will be handled. Privacy policies are outside the scope of this paper but see [14] for their derivation and use.
- The service is consumed by a person or another application accessing the service across the Internet.
- The consumer has security preferences for the e-service that may not be reflected in the provider's security policy.
- The consumer also has a privacy policy that defines what private information he is willing to give up and how that information is to be handled by the provider.
- There is usually a fee that the consumer pays the provider for use of the service.

Examples of current e-services are Amazon.com (online retailer), optionsxpress.com (online stockbroker), and WebMD.com (health information and technology solutions provider). Figure 1 shows a network view of an e-service.

2.2. Security policy requirements

Requirements for e-services security policies address what security measures should be covered in an e-service security policy. Since e-services fall under the category of open systems, we begin by looking at requirements prescribed by ISO 7498-2, the reference model for security architectures by the International Organization for Standardization [15].

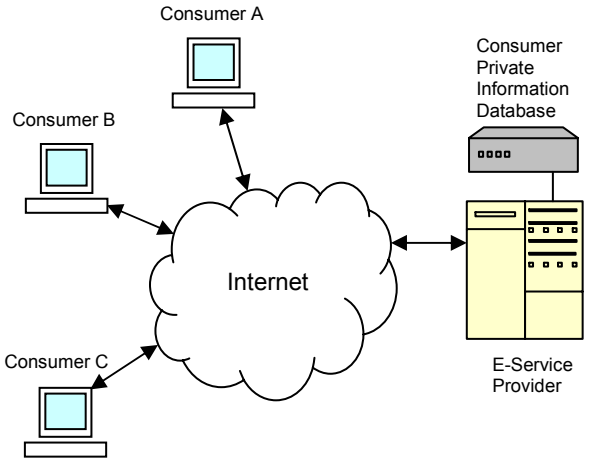

Figure 1. Network view of an e-service

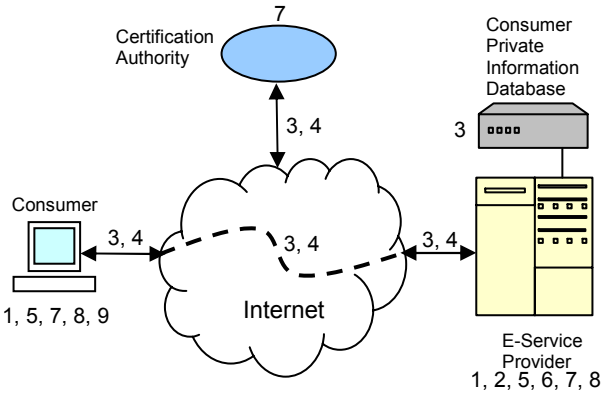

Figure 2. Application of security services (numbers correspond to security services in Section 2.2)

This standard identifies 5 main categories of security services:

1. Authentication
2. Access Control
3. Data Confidentiality
4. Data Integrity
5. Non-repudiation

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) provides Recommendation X.800, Security Architecture for OSI (Open Systems Interconnection) [16] that lists the same 5 main categories of security services as above. We propose that these 5 categories of security services be covered in an e-services security policy. We would add the following security services:

6. Secure Logging – of user transactions by the provider
7. Certification – user or provider would use some certifying authority to certify credentials
8. Malware Detection – user or provider would use some anti-malware software to detect and eliminate malware from their computing platforms
9. Application Monitoring – user platform monitoring for licensed, verified, and permitted applications

We thus have 9 security services that should be specified in an e-service security policy. Figure 2 identifies where these security services are typically applied using an e-service network view.

The above standards also list specific security services under the main security service categories. As an example, non-repudiation has the specific services (with the obvious meanings): "Non-repudiation, Origin" and "Non-repudiation, Destination". As well, security mechanisms (e.g. digital signature) are used to support security services, i.e. security policy requirements. We will employ specific services and security mechanisms to formulate our e-services security policy in Section 3.

2.3. Security policy negotiation requirements

Based on the nature of e-services and what goes on in negotiations in general, we propose the following requirements for e-services security policy negotiation:

1. The security measures to be negotiated must be clear and understandable.
2. The consumer may negotiate any subset of security measures in the policy.
3. There needs to be some form of trusted online help for the consumer in cases where it is difficult to know what choice to make in a particular step in the negotiation.
4. The consumer normally initiates negotiation after finding the e-service that he wants to use. However, when a provider changes its service and requires new security levels, it may initiate a security policy negotiation with the consumer.
5. Negotiation may be terminated by either the consumer or the provider, at any step in the negotiation prior to a successful outcome. If so terminated, the associated e-service may not proceed.
6. The user interface for the negotiation must be easy to use, intuitive, and trustable (i.e. give the user a sense of ease that everything is working as stated or planned).

Requirement 3 is needed in order that the negotiation is not blocked due simply to the fact that the consumer

does not know what security choice to make. This can occur quite easily where the consumer happens not to be security aware. We will propose a way for achieving this requirement in the next section.

3. Security policy negotiation for e-services

In this section, we define an e-service security policy according to the above security policy requirements. We then present an approach for e-service security policy negotiation that satisfies the above negotiation requirements.

3.1. E-Service security policy

Based on the requirements of Section 2.2, and using example values and security mechanisms, we propose the e-service security policy shown in Figure 3.

In Figure 3, the top shaded portion is the policy header. The header contains the following administrative fields: *policy use* identifies for which e-service the policy is provided, *owner* identifies the name of the provider of the e-service, and *valid* specifies the end date after which the policy is no longer valid, or "initial/continuing" which indicates whether or not the security policy is enforced only initially or continuously. The figure also shows that some security services can have multiple mechanisms (e.g. consumer authentication using password and biometrics). In such cases, the additional mechanisms can simply be listed under the security service. Note that security policy negotiation would involve the selection of a particular mechanism. Similarly, secure logging and access control can have additional items (e.g. access control can have additional resources under each role).

3.2. Security policy negotiation

We propose that security policy negotiation be the first of two stages of negotiation, the second stage being privacy policy negotiation. Privacy policy negotiation is fully described in [17, 18] and is outside the scope of this paper. Security policy negotiation is entered once the consumer has determined which e-service he wants to use. Privacy policy negotiation is entered only if security policy negotiation is successful. The e-service can only be activated if both stages of negotiation are successful. Where negotiation is not needed due to a match found between the provider's policy and the consumer's preferences, the match still signals a successful negotiation. Where a negotiation is unsuccessful, the consumer needs to look for another e-service to try (or find ways to match the security requirements of the e-service but it is probably easier to just find another e-service). Figure 4 gives a flowchart of this process.

Policy Use: E-learning *Valid:* unlimited	*Owner:* Learners Online, Inc.
CONSUMER PROVISIONS	**PROVIDER PROVISIONS**
Consumer Authentication *Implement:* yes (default) *Mechanism:* password *Mechanism:* V+F biometrics	**Provider Authentication** *Implement:* yes (default) *Mechanism:* security token *Mechanism:* digital signature
Consumer Non-Repudiation *Implement:* yes (default) *Mechanism:* digital signature	**Provider Non-Repudiation** *Implement:* yes (default) *Mechanism:* digital signature
Consumer Certification *Implement:* yes (default) *Mechanism:* certificate	**Provider Certification** *Implement:* yes (default) *Mechanism:* certificate
Consumer Malware Detect *Implement:* yes (default) *Mechanism:* Norton	**Provider Malware Detect** *Implement:* yes (default) *Mechanism:* Norton
Application Monitoring *Implement:* yes (default) *Mechanism:* IIT-ISG	**Data *S*tore Confidentiality** *Implement:* yes (default) *Mechanism:* 3DES encrypt
	Communication Confidentiality *Implement:* yes (default) *Mechanism:* SSL
	Communication Integrity *Implement:* yes (default) *Mechanism:* MD5 Hash
	Secure Logging *What:* order transactions *Mechanism:* 3DES encrypt *What:* user input *Mechanism:* 3DES encrypt
	Access Control *User Role:* Secretary *Resource:*scheduling module *Resource:* admin module *User Role:* President *Resource:* admin module *Resource:* salary module

Figure 3. E-Service security policy

In security policy negotiation (see Figure 5), a non-autonomous software agent acts on behalf of the consumer to receive/send negotiation messages from/to the provider. Another non-autonomous agent serves the provider in the same way. These agents also perform validation checks on the information to be sent.

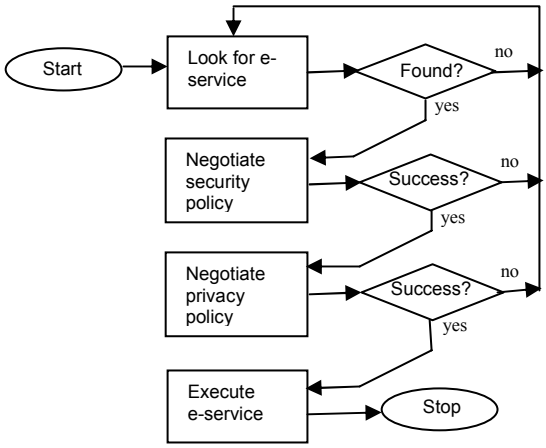

Figure 4. Stages prior to e-service execution

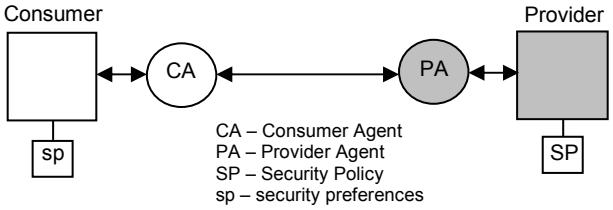

Figure 5. Security policy negotiation entities

Once the consumer has determined the e-service he wants to use, the security policy negotiation proceeds as follows (assuming a consumer-initiated negotiation):

1. The consumer requests the provider's security policy from the PA.
2. The consumer compares the provider's SP with his security preferences to see if there is a match. If there is a match, the CA signals a "successful negotiation" and the processing proceeds to privacy negotiation. If there is no match, consumer and provider begin security policy negotiation (step 3).
3. The consumer changes the provider's SP according to his/her preferences and sends it back (via the CA) to the provider. The provider either accepts the new SP or he/she changes it according to what he/she can accept. The provider then sends it back (via the PA) to the consumer. The consumer looks at it again and makes further changes and sends it back (via the CA) to the provider. This negotiation process continues back and forth until a) both sides agree and the negotiation is successful or b) one side terminates the negotiation (after concluding that no progress can be made) and the negotiation is unsuccessful. If the negotiation is unsuccessful, the consumer searches for another e-service to try (or tries to satisfy the provider's security requirements).

Figure 6 illustrates these steps using a message sequence chart for a consumer initiated negotiation (a provider initiated one would replace the top two arrows with one arrow from provider to consumer representing a request for negotiation together with the provider's SP). In Figure 6, SP1 is the consumer's first offer, SP2 is the provider's counter-offer, SP3 is the consumer's counter-counter offer and so on. After n steps the negotiation is successful, since the provider returns SPn, the consumer's last offer, unchanged.

We now examine the negotiation requirements of Section 2.3 to see how they can be fulfilled. Requirement 1 will be fulfilled in our prototype using online help in the form of pop-up windows that explain the particular security service for which help was requested.

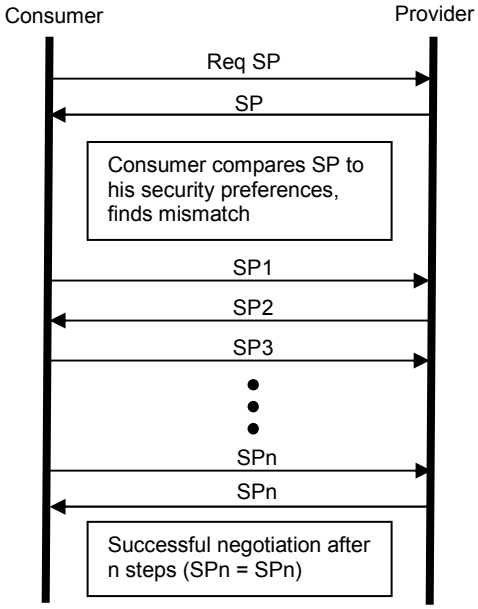

Figure 6. Security policy negotiation steps

Requirement 2 is fulfilled by the consumer's ability to change any subset of security measures in the policy. Requirement 3 is addressed below. Requirements 4 and 5 are already part of our negotiation procedure. Requirement 6 will be fulfilled in our prototype by an appropriate interface design. We will describe this interface in Section 4.

Scheme for online help in making offers

Negotiation requirement 3, the provision of trusted online help for the consumer to formulate a particular offer is fulfilled using the knowledge of what others selected under the same circumstances. This knowledge is acquired using the following steps:

1. Providers save and rank security policies that have been used with consumers. The ranking, for example, can be in terms of a security score $s = kv$ for each policy, where k is the number of security violations over the last 12 months (for example), and v is the average severity over all violations. Note that $s \geq 0$ is unbounded and the smaller the s, the better the associated security policy in the sense that it led to fewer security violations.
2. An e-services authority (EA) (could be a role for a PKI Certificate Authority) collects service provider security policies that have been used with various consumers, along with their security scores and the e-services to which they were applied. The EA anonymizes the security policies so that they cannot be identified with any particular provider or consumer.
3. In the course of a negotiation, a consumer who needs help in making a security choice (e.g. a security service or a security mechanism) can request from the EA the security policies matching the e-service and security scores below a certain threshold. The consumer would then use these policies to guide his/her choice.

This scheme clearly increases the workload of providers, but perhaps they would not mind doing it if they can advertise that they are doing this to help consumers, and thereby gain more business. This scheme also introduces a new role for an existing authority, such as a Certificate Authority. The authority can recover its costs by charging consumers a small subscription rate for providing this service.

3.3. Application to web services

The above approach for security policy negotiation applies to all e-services as defined in Section 2.1. We now examine how it can apply to web services.

Web services operate within a Service-Oriented Architecture (SOA) which uses XML, UDDI, SOAP, and WSDL to publish a service, find a service, and bind to a service [19]. In this scenario, a consumer wishing to execute a particular service would first find details of the service in the UDDI web services directory. (Providers would have previously populated the UDDI directory with details of the services they offer.) Once the consumer has sufficient information about the service, including service key and binding information, the consumer formulates a SOAP message to send to the provider to execute the service. It is here where our negotiation stages can be inserted. The initial SOAP message to the provider would not be to execute the service but to request the provider's security policy to begin the negotiation sequence. Only after the privacy policy negotiation is successful (with the negotiation stages as described in Section 3.2) would the SOAP message to execute the service be sent. Where a negotiation fails, the consumer would access the UDDI directory again to find another provider and start the negotiation stages all over again (or find ways to satisfy the provider's security policy).

Web services already possess XML-based language specifications to implement security policies and service level agreements. WS-Policy and WS-SecurityPolicy may be used to express web service security policies. WS-Policy may be applied to express security requirements for web services in general whereas WS-SecurityPolicy contains the policy elements applicable to WS-Security. WS-Agreement provides a language for expressing service level agreements between a web service provider and a web service consumer. However, none of these specifications define a negotiation protocol for the negotiation of security policies, as we have done in this work. Further, research is needed to see if WS-Agreement can be used to express security policy agreements. Finally, we have not as yet seen a full implementation of security policy negotiation as described in this work using these WS-* languages.

The use of the UDDI web services directory brings up an interesting possibility. Providers could store their security and privacy policies in addition to details of their service offerings in this directory. Consumers could then use the UDDI directory to select only those services that match their security preferences and privacy policies. This could lessen the need for negotiation (but not get rid of it entirely, as there may not be services that match completely) and result in fewer delays. However, the UDDI directory would need appropriate security protection, since successful attacks on this directory would be disastrous.

4. Prototype implementation

We have extended a prototype that we had developed for privacy policy negotiation [17, 18] so that it can be used for security policy negotiation. The prototype is based on a peer-to-peer architecture programmed in JADE (Java Agent Development Framework) [20]. The prototype allows a consumer

and a provider to contact each other across the Internet, initiate, and carry on a negotiation session. Only minor changes were needed to the prototype for security policy negotiation. The changes primarily involved a) provision of a pop-up window help facility for consumers who need to learn about a particular security service or mechanism (to satisfy requirement 1 of section 2.3), and b) enhancing the user selection mechanism to allow for selection of multiple choices needed for some security services such as authentication.

The main component of the user interface consists of a table (see Figure 7) that has columns for security service, implement (Y/N), and security mechanism. Figure 7 only

Security Service	Y/N	Security Mechanism
Consumer Authentication	Y	V+F Biometrics Certificate
Provider Authentication	Y	Certificate
Communication Confidentiality	Y	SSL VPN

Figure 7. Tabular interface of security policy negotiation prototype

shows 3 security services to keep it simple. A consumer can change the "Y" (default) to "N" to delete the associated security service. If the "Y" is left alone, the consumer can then select one or more of the corresponding security mechanisms.

For consumers who need help regarding what security choice to make during a negotiation session, the user interface provides this help by showing how many other security policies (corresponding to the same e-service and with security scores below the threshold) selected each choice by simply appending a number next to a choice (see Figure 8). Of course, the consumer must have previously requested help (via a button) and entered a security score threshold (Section 3.2). For example, Figure 8 shows that consumer authentication was selected in 15 security policies, whereas provider authentication and communication confidentiality were selected in 7 and 13 policies respectively. This guides the consumer to select consumer authentication as "a good security service to have" relative to the other two services. Similarly, within consumer authentication, the certificate mechanism is more popular than the biometrics mechanism. This guides the consumer into choosing certificate over biometrics. Although some of these choices (e.g. consumer authentication) may seem obvious to security knowledgeable people, we point out that we are targeting the general public with our approach and there are definitely people in this group who are not familiar with the choices. We expect to use this prototype in experiments to gage user reaction using volunteers. In so doing we hope to further improve our design for satisfying negotiation requirements 1, 3, and 6 of Section 2.3.

Security Service	Y/N	Security Mechanism
Consumer Authentication (15)	Y	V+F Biometrics (5) Certificate (10)
Provider Authentication (7)	Y	Certificate (7)
Communication Confidentiality (13)	Y	SSL (10) VPN (3)

Figure 8. Frequency of security attributes in other selected security policies

5. Conclusions and future work

We have presented our approach for security policy negotiation, including a scheme for providing online help to consumers who are not sure of what security choices to make. We showed how security policy negotiation can be used with web services that operate under the service-oriented architecture (SOA). Finally, we presented an overview of our prototype for security policy negotiation.

The novel contributions of this work include: a) an approach for security policy negotiation on a per consumer basis (even web services lack a negotiation protocol) integrated with privacy policy negotiation, b) a scheme for online help in making security policy offers during negotiation, and c) an interface for b) that easily and intuitively conveys the help needed. In addition, we have purposely kept our approach for a) simple, primarily so that the average consumer who is not a computer expert can understand how to use it. Any method, no matter how good, is doomed to failure if it is not used or not usable due to too much complexity.

Future research includes the following areas:

- Is the scheme for providing online help to consumers for making security choices feasible in terms of performance and scalability? What are

alternative ranking methods that can be employed to rank the security policies?

- We have been dealing with security for e-services but what about security for the security policies and the negotiations themselves? What kinds of protection are needed?
- For web services, how can WS-Policy, WS-SecurityPolicy, and WS-Agreement be used to specify security polices and agreements for our negotiation approach? How can we implement our negotiation protocol using SOAP? Is it feasible to use the UDDI directory to store provider security and privacy policies? What security measures are needed to protect the UDDI directory from attack?

References

[1] J. Joshi et al, "Security Models for Web-Based Applications", Communications of the ACM, Vol. 44, No. 2, pp. 38-44, February 2001.

[2] V. Varadharajan, "A Multilevel Security Policy Model for Networks", Proceedings, Ninth Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM 90), Vol. 2, pp. 710-718, June 3-7, 1990.

[3] S. Duflos, "An Architecture for Policy-Based Security Management for Distributed Multimedia Services", Proceedings, Multimedia '02, Juan-les-Pins, France, Dec. 1-6, 2002.

[4] P. Dinsmore et al, "Policy-Based Security Management for Large Dynamic Groups: An Overview of the DCCM Project", Proceedings, DARPA Information Survivability Conference and Exposition, 2000 (DISCEX'00), Vol. 1, pp. 64-73, Jan. 25-27, 2000.

[5] M. Ventuneac, T. Coffey, I. Salomie, "A Policy-Based Security Framework for Web-Enabled Applications", Proceedings, 1st International Symposium on Information and Communication Technologies, pp. 487-492, Dublin, Ireland, 2003.

[6] F. Barrere et al, "Inter-Domains Policy Negotiation", Proceedings, 4th International Workshop on Policies for Distributed Systems and Networks (POLICY'03), Lake Como, Italy, June 4-6, 2003.

[7] Y. Yang, Z. Fu, and S. Wu, "Bands: An Inter-Domain Internet Security Policy Management System for IPSEC.VPN", Proceedings, IFIP/IEEE Eighth Int'l Symposium on Integrated Network Management, March 2003.

[8] J. Park, J. Chung, "Design of SPS Model Using Mobile Agent System", Proceedings, IEEE 37th Annual 2003 Int'l Carnahan Conference on Security Technology, pp. 38-42, Oct. 14-16, 2003.

[9] H. Khurana et al, "Integrated Security Services for Dynamic Coalitions", Proceedings, DARPA Information Survivability Conference and Exposition (DISCEX'03), Washington D.C., U.S.A., April 2003.

[10] J. Hale et al, "Security Policy Coordination for Heterogeneous Information Systems", Proceedings, 15th Annual Computer Security Applications Conference (ACSAC '99), pp. 219-228, Dec. 6-10, 1999.

[11] E. Bertino, E. Ferrari, A. Squicciarini, "Trust Negotiation: Concepts, Systems, and Languages", Computing in Science and Engineering, pp. 27-34, July/August 2004.

[12] M. Winslett et al, "Negotiating Trust on the Web", IEEE Internet Computing, pp. 30-37, November/December 2002.

[13] W. Winsborough and N. Li, "Safety in Automated Trust Negotiation", Proceedings, 2004 IEEE Symposium on Security and Privacy (S&P'04), pp. 147-160, May 9-12, 2004.

[14] G. Yee, L. Korba, "Semi-Automatic Derivation and Use of Personal Privacy Policies in E-Business", *International Journal of E-Business Research*, Vol. 1, No. 1, Idea Group Publishing, 2005.

[15] International Organization for Standardization, "IS0 7498-2, Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture", as of Feb. 11, 2004, available from: http://www.iso.org/

[16] International Telecommunication Union Telecommunication Standardization Sector (ITU-T), "Recommendation X.800, Security Architecture for OSI", as of Feb. 11, 2004, available from: http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.800-199103-I

[17] G. Yee, L. Korba, "The Negotiation of Privacy Policies in Distance Education", Proceedings, 14th IRMA International Conference, Philadelphia, Pennsylvania, May 18-21, 2003.

[18] G. Yee, L. Korba, "Bilateral E-services Negotiation Under Uncertainty", Proceedings, The 2003 International Symposium on Applications and the Internet (SAINT2003), Orlando, Florida, Jan. 27-31, 2003.

[19] M. O'Neill et al, Web Services Security, McGraw-Hill / Osborne, 2003.

[20] Telecom Italia Lab, "JADE (Java Agent Development Framework)", available as of Feb. 14, 2005, from: http://jade.tilab.com/

[1] NRC Paper Number: NRC 47449