Personalized Security for E-Services

Yee, George

Publisher’s version / Version de l'éditeur:

Proceedings of The First International Conference on Availability, Reliability and Security (ARES 2006), 2006

National Research
Council Canada

Conseil national
de recherches Canada

Institute for
Information Technology

Institut de technologie
de l'information

NRC · CNRC

Personalized Security for E-Services *

Yee, G.

April 2006

* published in the Proceedings of The First International Conference on Availability, Reliability and Security (ARES 2006). April 20-22, 2006. Vienna, Austria. NRC 48463.

Canada

Personalized Security for E-Services[1]

George Yee
Institute for Information Technology
National Research Council Canada
george.yee@nrc-cnrc.gc.ca

Abstract

The growth of the Internet has been accompanied by a proliferation of e-services. The increasing attacks on these services by malicious individuals have highlighted the need for security. The security requirements of an e-service may be specified by the service provider in a security policy. However, a service consumer may have security preferences that are not reflected in this policy. In order for service providers to reach a wider market, a way of personalizing a security policy to a particular consumer is needed. We introduce the concept of security personalization, derive the content of an e-service security policy suitable for personalization, and describe four approaches for such personalization, including the design and use of a context-aware security policy agent (CASPA) that personalizes an e-service security policy to the needs of the consumer on-the-fly. We further give recommendations on applying the personalization approaches based on their advantages and disadvantages.

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.

The objectives and contributions of this paper are to a) introduce the need for personalization of service provider security policies, b) derive an example e-service security policy suitable for personalization, c) describe different approaches for personalizing an e-service security policy, including the design and use of a context-aware security policy agent (CASPA) that personalizes an e-services security policy to the needs of the consumer on-the-fly, and d) give recommendations on how to apply the personalization approaches to e-services.

An e-service provider makes use of a security policy to specify the security measures that it has put or will put in place to protect its e-services. However, this security policy may not match up with the security preferences of a potential consumer of an e-service. 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 or needs is to allow the security policy to be personalized to the consumer, reflecting the consumer's preferences and needs.

The goals of personalizing security for e-services include a) to make it attractive (or possible) for consumers to utilize the e-service by adding security flexibility, as illustrated in the examples above, and b) to upgrade security (e.g. adding biometric authentication) when an upgrade is needed, or to downgrade security (e.g. substituting 3DES encryption for AES encryption) when a downgrade makes sense (e.g. mobile device with low computing power) and leads to better performance.

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.

There is a large body of literature on personalization, that regards personalization primarily as website personalization for e-commerce, where a site's configuration is customized to the user's interaction preferences, based on feedback data covering, for example, user navigation style and buying habits. Adomavicius and Tuzhilin [6] discuss various personalization technologies for this purpose. Wu et al [7] present a classification scheme for personalization used on e-commerce websites. This is not to say that personalization has not been applied elsewhere. In fact, Bertino et al [8] describe personalizing call routing for telecommunications and Panayiotou & Samaras [9] discuss the use of agents to personalize portals for wireless users, arguing that wireless and mobile users have information access and service needs that are very different from those of the desktop user. In addition, Rykowski, & Cellary [10] describe the use of software agents to personalize web services into a "virtual web service", a collection of linked real web services and/or virtual web services and agents accessed as a single real web service. Our last examples of personalization are the works of Teevan et al [11], who studied web search algorithms that take into account a user's prior search interactions to personalize the user's current search, and Zhiwen et al [12], who presented an agent-based adaptive television program system for personalized TV viewing. We conclude that personalization of online content is not new and has been applied in many areas. However, we were unable to find any work that deals with personalizing security for e-services as proposed here.

The remainder of this paper is organized as follows. Section 2 defines e-services and derives requirements for security policies. Section 3 describes four approaches for security policy personalization, highlighting some of the advantages and disadvantages of each approach. Section 4 presents recommendations for applying the personalization approaches. Finally, Section 5 presents our conclusions and areas for future research.

2. E-Services and requirements for security policies

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 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.
- 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 [13]. This standard identifies 5 main categories of security services:

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

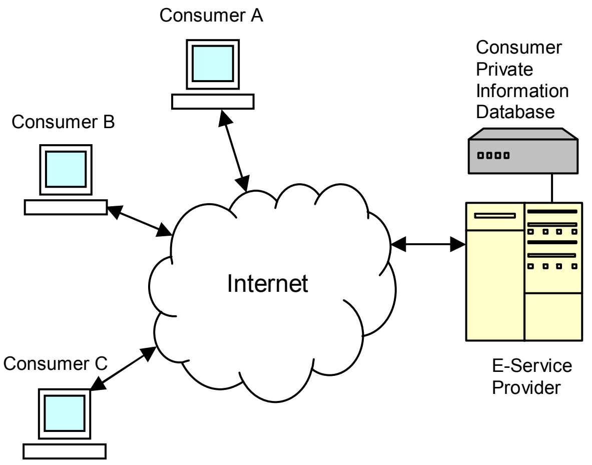

Figure 1. Network view of an e-service

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) provides Recommendation X.800, Security Architecture for OSI (Open Systems Interconnection) [14] 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 below.

2.3. E-Service security policy

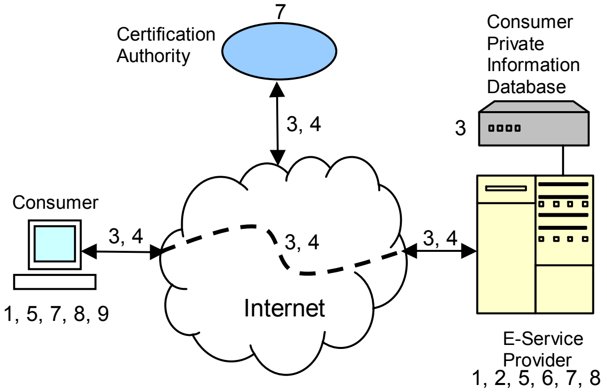

Figure 2. Application of security services (numbers correspond to security services in Section 2.2)

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

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. Similarly, secure logging and access control can have additional items (e.g. access control can have additional resources under each role). Note that security policy personalization would involve the selection of particular security services and mechanisms or the addition / deletion of certain security services and mechanisms, according to the needs of the e-service.

Our example e-services security policy serves as a model or template from which new security policies can be obtained through personalization.

3. Approaches for security policy personalization

Four approaches to personalizing an e-service security policy are: 1) selection from a pre-defined screen, 2) policy negotiation, 3) use of CASPA, and 4) combination of policy negotiation and use of CASPA.

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 Store 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. Example e-service security policy

The descriptions of each approach along with some attending advantages and disadvantages follow.

3.1. Selection from a pre-defined screen

This is the simplest of the four approaches and the easiest one of the four to implement. Upon engaging an e-service, the consumer is presented with a screen in which she can select the security services and mechanisms for the ensuing e-service. This screen can be a representation of the provider's security policy for the e-service, with content similar to Figure 3. This approach is similar to setting the security levels for an Internet browser such as Microsoft's Internet Explorer. The user interface of the screen can include pop-up windows containing help information to guide the selection process. The help information can itself be personalized to the user in terms of user experience and knowledge, e.g. beginner, intermediate, and advanced. The screen can execute at the provider's website or on the user's e-service platform (e.g. mobile device or desktop PC) via an applet. Some advantages of this approach are: a) easy to implement since selection of items from a web page is a well-known and proven technology, and b) high user acceptance, since the user is most likely already familiar with such a selection process, which is commonly found on the Internet. A serious disadvantage is that the user is limited to the security choices provided by the e-service provider, so it is not true or full personalization.

3.2. Policy Negotiation

In security policy negotiation [15] (see Figure 4), 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.

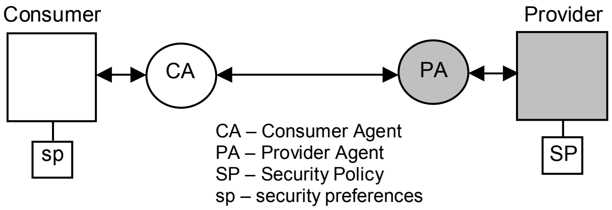

Figure 4. Security policy negotiation entities

Once the consumer has determined the e-service she 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 her security preferences to see if there is a match. If there is a match, the CA signals a "successful negotiation" and the e-service may begin (there is actually a privacy policy negotiation step after security policy negotiation [15] but we omit this here to focus on security). If there is no match, consumer and provider begin security policy negotiation (step 3).
3. The consumer changes the provider's SP according to her preferences and sends it back (via

the CA) to the provider. The provider either accepts the new SP or she changes it according to what 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). If the negotiation is successful the e-service may begin.

Some advantages of this approach are: a) fuller personalization – the consumer can negotiate security services or mechanisms that the provider never intended, and b) can render an e-service that was unusable (e.g. access restrictions) usable (e.g. negotiated access options). Some disadvantages are: a) can be more complicated and difficult to use if the user interfaces are not properly designed, and b) requires a fairly knowledgeable user who knows what security measures she needs.

3.3. Use of CASPA

A context-aware security policy agent (CASPA) is an intelligent software agent that resides in a consumer's e-service platform (e.g. mobile device such as a wireless PDA) and is responsible for selecting security services and mechanisms from the provider's security policy for a particular e-service, according to the values of UPL (the context) for the consumer's e-service platform, where U represents user security preferences, P represents the power level of the platform, and L represents the platform's location. P and L are mostly applicable only to mobile e-service platforms. L is used to detect dangerous areas containing high attacker activity. Note that the provider's security policy has to be capable of being personalized, similar to the policy in Figure 3, and both consumer and provider must agree to use the policy for the e-service.

CASPA behaviour. The behaviour of a CASPA is described by the state machine in Figure 5, where the arrow labels are in the form "condition / action".

In Figure 5, the *Idle* state is exited once the service is ready to begin (i.e. the service has been found and the security policy agreed to between consumer and provider).

In the *Initialization* state, the CASPA accounts for the U and P of UPL (i.e. reflects the user's security preferences and the computational power of the e-service platform) by setting the options in the provider's security policy to implement appropriate security services and mechanisms (see Figure 3). For example, suppose the consumer has several mobile platforms that she uses with the same security policy, including a PDA and a less powerful cell phone. CASPA would set security services and mechanisms that both reflect the consumer's security preferences and be appropriate to the computing power of each platform. It should be straight forward to program a CASPA to perform this task. Once its work in the *Initialization* state is completed, the CASPA transitions to the *Idle* state if the e-service platform is non-mobile; otherwise, it transitions to the *Monitor Location* state.

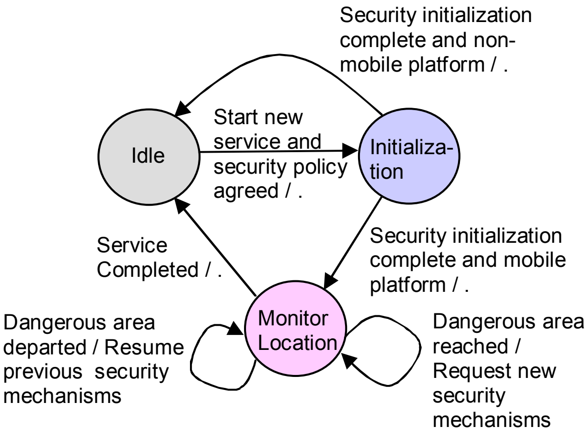
Security initialization complete and non-mobile platform / .
Idle
Start new service and security policy agreed / .
Initialization
Security initialization complete and mobile platform / .
Service Completed / .
Monitor Location
Dangerous area departed / Resume previous security mechanisms
Dangerous area reached / Request new security mechanisms

Figure 5. Behaviour of CASPA

In the *Monitor Location* state, the agent is monitoring the mobile platform's location using GPS. Note that this location is only used by the CASPA and is not reported to either the mobile ISP (Internet Service Provider) or the provider of the service so that there should be no privacy concerns (more on this below). An alternative way of determining the consumer's location is the use of signaling analysis by the mobile ISP. However, the latter would then learn the consumer's location leading to privacy concerns. When a dangerous area (i.e. an area with a high number of attackers) is entered, the agent messages the service provider to initiate a more powerful security mechanism for communication to defend against the attackers (how this dangerous area can be known is discussed below). Of course, this more powerful mechanism consumes more computing resources and should only be used when necessary. When the dangerous area is exited, the agent messages the provider that the normal security mechanism for communication may be resumed. The CASPA executes concurrently with the e-service. However, the e-service does not begin until the security initialization has been completed (CASPA has transitioned out of the *Initialization* state).

Communication with the e-service provider. The CASPA communicates with the provider during *Initialization* and *Monitor Location* using the following secure protocol:

1. $C \rightarrow P: Sig_C (M, nonce)$
2. $P \rightarrow C : Sig_P (nonce-1)$

where C is the consumer, P is the provider, Sig_C is the consumer's digital signature, Sig_P is the provider's digital signature, M is the message, and the nonce is used to prevent replay attacks and as a confirmation of receipt by the provider.

For *Initialization*, the message M has the form:

M = [INIT, security component 1, security component 2, ..., security component k],

where *security component j = security service j,* if this security service has no alternative security mechanisms, or *security component j = (security service j, mechanism idj),* if it has alternative mechanisms and *mechanism idj* is the mechanism the user wants.

For Monitor Location, upon entering the dangerous area, the message M has the form:

M = [NEW, (security service 1, mechanism id1), (security service 2, mechanism id2), ..., (security service m, mechanism idm)]

which sets the new mechanism of each security service that the consumer wants to implement for the dangerous area, for appropriate security services having alternative mechanisms. As we have alluded to above, in most cases the only security services of concern would be communication confidentiality and integrity. Upon exiting the dangerous area, the message M is: *M = [REVERT]* which tells the provider to revert to the previous mechanisms.

Operational requirements and discussion. The CASPA would need to know the user's security preferences, including the preferences corresponding to P and L from UPL, in order to formulate the messages *M*. These could be input via a UI for the CASPA. This information can be provided by the consumer once before any e-services are used, and then verified with the agreed-to security policy for each service. The security preferences in *M* have to be realizable within the agreed-to security policy. In addition, the agreed-to security policies need to be expressed in a machine processable language such as XACML (eXtensible Access Control Markup Language) [16].

The provider needs to have software to receive the messages from the CASPA and apply them to the e-service's security policy. This software could take the form of an agent as well, a counterpart to CASPA that acts on behalf of the provider.

In the *Monitor Location* state, an appropriate UI would be needed to interrupt the service temporarily while one or more security mechanisms are changed. This interruption occurs twice – once for entering the dangerous area and once for departing the dangerous area. Further, these changeovers need to occur quickly, in order not to annoy the user and to prevent any openings for attack. Dangerous areas may be determined as a result of feedback to a government website by users who have been attacked. The CASPA can periodically and automatically check this website for the latest dangerous areas.

The location obtained using GPS is only used by the CASPA and not reported to the providers which should not lead to privacy concerns. However, the dangerous areas are known to the e-service provider as well. The latter may infer the location of the consumer when the CASPA signals for higher security. We assume that this small breach of privacy is acceptable to the consumer in return for greater security, since the consumer's location may not be pinpointed exactly due to the possibility of more than one dangerous area and the fact that the consumer may enter a dangerous area at many different locations.

Our use of digital signatures and nonces implies that a mobile platform needs at least the capability to process a digital signature and generate random numbers. In addition, there would need to be a key distribution technique, as well as the capability for the platform to securely store a private key. However, these are minimal capabilities required to implement security services. Further, we require the mobile platform to have a GPS capability, which is becoming more and more common. These requirements imply that a mobile platform should probably have the computing power of a PDA. However, less powerful platforms would be accommodated by the CASPA where possible.

We note that since the security policy is executed by the provider of the e-service, the mobile e-service consumer can transparently use different mobile ISP's as she roams with her mobile platform.

Some advantages of using CASPA for security policy personalization are: a) provides dynamic personalization on-the-fly, b) accounts for platform power level and location for mobile e-service platforms, and c) straight-forward to implement. Some disadvantages are: a) can be difficult to use if the user interfaces are not properly implemented, and b) requires a security knowledgeable consumer who knows what security measures she needs.

3.4. Combination of policy negotiation and use of CASPA

In this combined approach, the security policy for use with a CASPA is obtained by using policy negotiation. The approach may be termed *double personalization* since security is first personalized by negotiation, and then personalized again on-the-fly by the CASPA. The advantages and disadvantages here are the combined advantages and disadvantages of policy negotiation and the use of CASPA.

4. Application of security personalization approaches

The above security personalization approaches may be used for various types of e-services and consumers based on their advantages and disadvantages. An e-service that has limited variability in terms of the way it is used or in terms of the security expectations of its consumers may be satisfactorily matched with the pre-defined screen approach. For example, purchase services provided by eBay.com fall into this category. On the other hand, an e-service that has large variability in terms of these parameters may be better suited to the combination approach. For example, e-learning services fall into this latter category. The number of ways of using e-learning can be highly variable both in terms of the e-service platform and in terms of the application area. The consumer security expectations for e-learning can also be highly variable and can range from nearly no security needed for publicly available university courses to very high security needed for secret defense training.

Table 1 gives our recommendations for applying the personalization approaches to e-services by characterizing e-services in terms of the above mentioned variability and using the strengths and weaknesses of each approach. For example, the pre-defined screen approach allows limited security choices and therefore corresponds to low variability in number of ways to use the service and low variability in security expectations. To decide which personalization approach to use for a particular e-service, determine the table column values for the e-service and select the approach corresponding to the higher value (or equal value if both values are equal). For example, if variability in number of ways is low and variability in expectations is high, select the combination approach. Deciding between negotiation and CASPA may be a challenge since both are assigned "medium". Here, other factors may be used to break the tie, such as whether or not the e-service platform is mobile (choose CASPA) or if new security services need to be added to the policy (choose negotiation). If such tie-breaking factors do not exist, choosing either one should not cause any problem. Note that security expectations are linked to security knowledge, i.e. the higher the expectations, the higher the knowledge. Table 1 also shows that the personalization approaches nicely cover the full range of e-services in terms of the two column values.

Table 1. Application of personalization approaches

Personalization Approach	Variability in Number of Ways of Using the E-service	Variability in Consumer E-Service Security Expectations
Pre-defined Screen	Low	Low
Policy Negotiation	Medium	Medium
Use of CASPA	Medium	Medium
Combination Negotiation and CASPA	High	High

5. Conclusions and future research

We have introduced the concept of security policy personalization, derived an example e-service security policy that can be personalized, presented four approaches for security policy personalization, and given recommendations for applying the approaches. Security personalization approaches are expected to increase the attractiveness of e-services so that they can reach a wider audience.

The novel contributions of this work include: a) derivation of an example e-services security policy that can be personalized, b) novel approaches for security policy personalization, i.e. the negotiation, CASPA, and combination approaches, and c) recommendations for applying the personalization approaches.

Future research includes investigating the following questions: a) What are other approaches for personalization? What are other ways of determining when and what personalization to apply? b) We have been dealing with security for e-services but what about security for the security policies and the personalization methods themselves? What kinds of protection are needed? c) How can the personalization approaches be implemented in a web services environment making use of the web services protocols such as WSDL, SOAP, WS-Policy, WS-SecurityPolicy, and WS-Agreement?

References

[1] J. Joshi, W. Aref, A. Ghafoor, & E. Spafford, "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, D. Balenson, M. Heyman, P. Kruus, C. Scace, & A. Sherman, "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] G. Adomavicius, A. Tuzhilin, "Personalization Technologies: a Process-Oriented Perspective", Communications of the ACM, Vo. 48, Issue 10, pp. 83-90, October 2005.

[7] D. Wu, I. Im, M. Tremaine, K. Instone, M. Turoff, "A Framework for Classifying Personalization Scheme Used on e-Commerce Websites", Proceedings of the 36th Annual Hawaii International Conference on System Sciences, January 2003.

[8] E. Bertino, M. Mesiti, M. Cochinwala, "A Trigger-Based Approach for Communication Personalization", Proceedings of the International Database Engineering and Applications Symposium (IDEAS'04), pp. 3-13, July 2004.

[9] C. Panayiotou, G. Samaras, "mPERSONA: Personalized Portals for the Wireless User: An Agent Approach", Mobile Networks and Applications, Vol. 9, Issue 6, pp. 663-677, December 2004.

[10] J. Rykowski, W. Cellary, "Virtual Web Services – Application of Software Agents to Personalization of Web Services", Proceedings of the Sixth International Conference on Electronic Commerce (ICEC'04), 2004.

[11] J. Teevan, S. Dumais, E. Horvitz, "Personalizing Search via Automated Analysis of Interests and Activities", Proceedings of the 28th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 449-456, Salvador, Brazil, 2005.

[12] Y. Zhiwen, Z. Xingshe, S. Xiaowei, G. Jianhua, A. Morel, "Design, Implementation, and Evaluation of an Agent-Based Adaptive Program Personalization System", Proceedings, Fifth International Symposium on Multimedia Software Engineering, pp. 140-147, 2003.

[13] 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/

[14] 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

[15] G. Yee, L. Korba, "Negotiated Security Policies for E-Services and Web Services", Proceedings, 2005 IEEE International Conference on Web Services (ICWS 2005), Orlando, Florida, July 11-15, 2005.

[16] OASIS, "eXtensible Access Control Markup Language", available as of Sept. 10, 2005 from: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[1] NRC Paper Number: NRC 48463