Chapter 9
Security Personalization for
Internet and Web Services

George O.M. Yee
National Research Council Canada, Canada

Larry Korba
National Research Council Canada, Canada

ABSTRACT

The growth of the Internet has been accompanied by the growth of Internet services (e.g., e-commerce, e-health). This proliferation of services and the increasing attacks on them by malicious individuals have highlighted the need for service security. The security requirements of an Internet or Web service may be specified in a security policy. The provider of the service is then responsible for implementing the security measures contained in the policy. However, a service customer or consumer may have security preferences that are not reflected in the provider’s security policy. In order for service providers to attract and retain customers, as well as reach a wider market, a way of personalizing a security policy to a particular customer is needed. We derive the content of an Internet or Web service security policy and propose a flexible security personalization approach that will allow an Internet or Web service provider and customer to negotiate to an agreed-upon personalized security policy. In addition, we present two application examples of security policy personalization, and overview the design of our security personalization prototype.
INTRODUCTION

The term “Internet service” is used here to mean any electronic service that is accessed using the Internet, for example electronic banking. In the following, we use “Internet service” to refer to all electronic services that are available through the Internet, including Web services that are based on the service oriented architecture. We use “Web service” when we wish to indicate that we are treating Web services in particular.

A large number of Internet services targeting consumers have accompanied the rapid growth of the Internet. Internet services are available for banking, shopping, learning, healthcare, and the 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 (Joshi, Aref, Ghafoor, & Spafford, 2001).

In order for Internet 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 these services is to make use of security policies. An Internet service security policy is a specification of what security measures will be used to protect the 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 article.

An Internet 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 services. However, this security policy may not match up with the security preferences of a customer or consumer (we use “user,” “customer,” and “consumer” interchangeably) of the services. For example, suppose the security measure is user authentication via password. This authentication approach is known to be insecure. A security-sensitive consumer such as a defense contractor, may wish to add biometric authentication. Unless the user authentication is changed to include biometrics, the defense contractor would not be able to make use of the service. As another example, suppose the security measure is access control. The provider’s security policy may provide access to five features of a service, whereas a particular customer may need access to only three features. In this case, the customer may be reluctant to make use of this provider’s service, especially if the customer 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 customer’s security preferences is to allow the customer to personalize the security policy by negotiating with the provider regarding the security measures that are in the provider’s security policy. We call this negotiation process security policy personalization, that is, the provider’s security policy becomes personalized to a particular customer through negotiation.

This article extends Yee & Korba (2005b) by: (a) providing new details on the “scheme for online help in making offers” during the negotiation process, (b) providing new details on how the approach can be implemented for Web Services, (c) giving a more complete description of the prototype, (d) adding example applications, (e) enlarging the section on related works, (f) including an evaluation of the proposed approach for security policy personalization, and (g) improving the clarity of the writing in all sections.

The objectives and contributions of this article are to: (a) introduce the need for personalization of provider service security policies, (b) derive a security policy template suitable for use with Internet services, (c) present an approach for consumer-provider negotiation that accomplishes this personalization, including a novel method of providing help during negotiation, (d) show how security policy personalization can be implemented for Web services, (e) give example applications of security policy personalization, (f) describe our prototype for security policy negotiation, and (g) evaluate this work and discuss related works.
Related Content

Development of a 4D Visualization Tool for Construction Planning
[www.igi-global.com/chapter/development-visualization-tool-construction-planning/53270?camid=4v1](www.igi-global.com/chapter/development-visualization-tool-construction-planning/53270?camid=4v1)

Karma2: Provenance Management for Data-Driven Workflows
[www.igi-global.com/article/karma2-provenance-management-data-driven/3117?camid=4v1](www.igi-global.com/article/karma2-provenance-management-data-driven/3117?camid=4v1)

RAW Architecture: Reflective and Adaptable Web Service Model
[www.igi-global.com/article/raw-architecture-reflective-adaptable-web/3054?camid=4v1](www.igi-global.com/article/raw-architecture-reflective-adaptable-web/3054?camid=4v1)

Introduction to Web Services
[www.igi-global.com/chapter/introduction-web-services/28883?camid=4v1](www.igi-global.com/chapter/introduction-web-services/28883?camid=4v1)