CardSpace in the Cloud (Poster)

David W Chadwick
University of Kent
School of Computing
Canterbury, Kent, UK
+44 1227 82 3221
d.w.chadwick@kent.ac.uk

George Inman
University of Kent
School of Computing
Canterbury, Kent, UK
+44 1227 82 3221
G.Inman@kent.ac.uk

Paul Coxwell
Voice Commerce Group
Great Shelford
Cambridge, UK
+44 1223 550920
paul.coxwell@voice-commerce.com

ABSTRACT

This paper describes a web based federated identity management system which is based on the user centric approach of the Information Card model, and has been enhanced to remove many of the problems inherent in Microsoft's original design. Furthermore the new design is adapted to interwork with existing SAML 2 federations. Our model supports not only improved user mobility and the aggregation of claims from multiple identity providers (IdPs), but also user authentication via just one of the IdPs without placing any constraints on the authentication mechanism that is used. This is achieved by introducing a new component, the Linking Identity Selector, which allows the user to select multiple cards at service provision time. Users can then use the combined set of credentials to access a wider range of web based resources. We describe our first example application which allows the user to present a credit card, a self asserted card, a hotel loyalty card and a frequent flyer card in order to make an online hotel booking, using voice biometrics for authentication.

Categories and Subject Descriptors

D.4.6. Security and Protection, Access Controls

General Terms

Design, Security.

Keywords

Information Cards, Attribute Aggregation, CardSpace, Voice Authentication, Federated Identity Management, Authorisation.

1. INTRODUCTION

Information cards are a core component of Microsoft's Cardspace identity management and authorisation system. A good high level overview of CardSpace can be found in [1]. Each information card is a partial representation of a user's online digital identity and the full set of cards is a representation of the user's entire digital identity. Information Cards have some excellent features in terms of usability and security. From a usability perspective InfoCards provide a metaphor that is familiar to users i.e. that of plastic cards in a wallet. The simple clicking of a card simultaneously provides user consent and submission to a service provider (SP). Cards may be self issued or managed, meaning that the claims originate from either the user herself or an Identity Provider (IdP). From a security perspective they significantly reduce the risk from phishing attacks, they provide privacy protection of the user's personal information, and good assurance to the service provider (SP) that the user does have the attributes or claims that are being asserted. Unfortunately the model suffers from a number of significant disadvantages. CardSpace only supports a limited number of authentication mechanisms with an IdP (un/pw, X.509 certificate and Kerberos V5) and adding new mechanisms such as voice biometrics or one-time passwords is impossible without significant changes to the protocol flows. The user's cards are held in a fat client on the desktop (the Identity Selector) which constrains mobility and limits the choice of end user devices. Furthermore, Cardspace only allows a single card to be used in each transaction. This is a serious limitation, since in the physical world of plastic cards, users typically have lots of cards issued by many different IdPs, with each card typically holding only one (or very few) user attribute(s), along with its validity period, a user identifier, a mechanism to authenticate the user (usually a signature or PIN, but could be a photograph as well), and details of the issuer. Other contents such as holograms and chips are there to ensure the authenticity of the physical card and the attribute assertion (or claim) that it makes. They do not provide additional attributes of the user. Thus as federated identity management systems expand to Internet scale, users will need to aggregate their attributes from multiple IdPs. In the InfoCard model this means that users will need to be able to select and use multiple cards in a single transaction.

By way of a motivating example, we present the use-case of a user wishing to make an online hotel booking, in which she needs to prove she has a valid credit card, she wishes to present her hotel loyalty card to get a free room upgrade, her frequent flyer card to score air miles, and her current name and address (which are different to those registered with the various card holders). Furthermore, the user does not wish to have to remember lots of usernames and passwords, and because she is sending her credit card details, she wants to use her credit card IdP which uses strong authentication. In our case the credit card IdP offers voice biometrics to authenticate her. It also offers the protection option of not revealing her credit card details to the hotel, but instead sending it an assertion with a session identifier confirming that the user holds a valid credit card, and that payments can be charged to the session id.

CCS'10, October 4-8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

2. CONCEPTUAL MODEL

Our model assumes that the user is the only person who knows about all of her managed cards (i.e. IdP accounts), and that *she does not wish any IdP to know about all of her other accounts. This mirrors real life today.* We further assume that all IdPs and SPs are part of a pre-existing federation structure with pre-existing trust relationships between them. We introduce a new SP into the federation, called a Linking Identity Selector (LIS). *The LIS holds links to the user's various IdP accounts, and allows the user to select multiple cards (IdPs) at service provision time*. The LIS helps to protect the privacy of the user since the IdPs link to the LIS instead of to each other. Furthermore *the LIS does not have any knowledge of who the user actually is or what attributes are held by each individual IdP, except for those attribut*e types (but not values) that the user chooses to release to the LIS when she links her accounts together. The user is free to choose any LIS in the federation and is not bound to any single provider. The user may have different accounts at multiple LISs if desired. Each LIS is trusted by the IdPs and SPs to hold the user's account information confidentially and securely and to only release details back to their respective IdPs and to SPs when requested by the user.

2.1 IdP/Card Registration

We introduce a pared down InfoCard schema *that contains no personal data*, only the picture/logo and name of the IdP along with the metadata needed to access it. *The advantage of this design is that a single InfoCard is valid for all users, and cards can be made publically available.* If they are intercepted or lost they don't affect the user's privacy (unlike current InfoCards). We further propose that *each IdP hosts an InfoCard well known address* e.g. http://idp.com/InfoCard/ where users can obtain cards. This removes a current limitation of today's managed cards, i.e. no-one knows how or where to get them. When a user wishes to retrieve an InfoCard as a file she can navigate to this well known address using any browser and download it to her PC.

Since our Identity Selector runs in the cloud, *there is no reason for users to need to import and export their cards as they move between devices*, as with current InfoCards, since all their devices can contact the LIS in the cloud. *Users access the LIS with a normal web browser and a simple new plug-in module*, which is advantageous to using the thick client of current CardSpace systems.

The user may upload one of her InfoCard files to the LIS, or the LIS may already hold cards for all the IdPs in the federation. Once the LIS knows which card the user wishes to use, it will redirect the user to the authentication service of that IdP, using the metadata on the card. This will prompt the user to login/authenticate using any mechanism it chooses. *We thus devolve the act of authentication from the identity selector, thereby freeing the IdPs to use any authentication mechanisms they wish.* In the pilot scheme we are constructing, our Credit Card IdP, run by Voice Commerce Group, will be using voice biometrics to authenticate users. We use the standard SAMLv2 protocol [2] for interactions between the user's browser, the LIS (acting as SP) and the IdP, although an alternative protocol mapping could be devised if desired.

The LIS requests an authentication and attribute token from the IdP, which should contain a random but persistent identifier (PId) for this user. This PId is used as a pair-wise secret between the LS and the IdP to identify the user's account at either end in all future communications between the two parties. After authenticating the user, the IdP asks the user which attribute types she wants to include in her linked card at the LIS, and includes these in the response. When the LIS receives an unknown PId, it creates a new account for the (unknown) user in its internal database and stores each of the returned attribute types in the user's card for this IdP. These attribute types are used to dynamically determine which IdPs are selectable at service provision time. When the LIS receives an existing PId, it locates the (unknown) user's existing account in its database. If the user wishes to link additional IdP accounts to her existing LIS account then she submits or chooses another IdP card and is redirected to that IdP. The LIS requests another PId and set of attribute types from this IdP and adds these to the same LIS account.

We have also built support for the NIST Level of Assurance (LoA) [3] into our conceptual model, as described in [4], but space limitations prevent us from detailing it here.

2.2 Service Provision

In order to provide a web based Identity Selector that is interoperable with existing CardSpace SPs we introduce a thin client module that is pluggable into the user's web browser. This module is used to discover the user's LIS, to redirect the user there, and finally to return the (possibly aggregated) claims to the SP as in the existing CardSpace system. The only difference with current systems is that multiple cryptographically linked claims from multiple IdPs may now be provided to the SP.

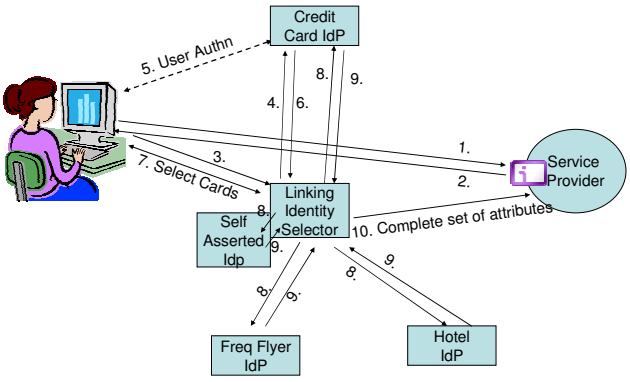

Figure 1. Service Provision Protocol Interactions

The user navigates to an InfoCard enabled HTML page at the SP's site and clicks on the InfoCard icon using their browser (step 1). The returned page (step 2) contains an embedded InfoCard MIME object that causes the browser to invoke our new plug-in module rather than the fat Identity Selector from Microsoft. The module downloads the SP's security policy which is parsed to determine the set of attribute types required to access the service. *We have defined an enhanced security policy that allows multiple IdPs with different attribute claims to be specified.* This is a significant enhancement to the CardSpace framework. The module next discovers the location of the user's LIS in one of two ways. The user may bookmark the home page of her LIS in a

reserved bookmarks folder that can be accessed by the module. The module can then display this/these bookmarks to the user and let her choose her preferred LIS. Alternatively the user can directly enter a URL into the module (see Figure 2). *This allows our system to be used on any Internet café computer without releasing personal information to other users. Our system prevents phishing attacks since a fraudulent SP is not able to redirect the user to a LIS of its own choosing.*

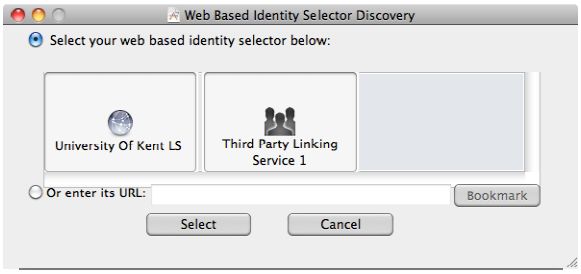

Figure 2. The LIS Discovery Mechanism

When the user has selected their LIS, the module establishes an SSL connection with it to protect all future communications between the browser and the LIS (step 3). The module requests the set of claims required by the SP from the LIS and asks that the attributes be returned encrypted for the SP. When the LIS receives this message it acts as a Where Are You From (WAYF) service and displays a page to the user showing her a list of all the IdPs that it has trust relationships with. The user chooses one of these IdPs (at which she has an account) and is redirected there (step 4). In our case the user chooses her credit card IdP.

The user is now invited to authenticate to the IdP using its supported mechanism(s) (step 5). In the IdP we are developing, the user enters her email address to this page, the IdP looks this up in its database, then rings the registered mobile phone number and asks her to speak a phrase. The voice biometrics used by our IdP strongly authenticate the user.

The IdP responds to the LIS by returning an authentication assertion containing a random session ID and a "referral" attribute which contains the user's PId encrypted for the LIS (step 6). The LIS is able to decrypt the PId and access the user's account. It displays all the user's cards in an Identity Selector like page (step 7). The page comprises three windows, the bottom two being similar to today's Identity Selector, and having similar functionality. The top window contains cards that have already been selected, the middle window shows cards that have previously been sent to this SP (but not yet selected), whilst the bottom window shows cards that have never been sent to this SP. This tells the user to exercise extra care if she decides to send any of these cards to this SP. Those cards that match the SP's requirements are lit up and those that don't are greyed out (and not selectable). The top window initially only contains one card, that of the authenticating IdP. As the user clicks on cards in either of the two lower windows two things happen. Firstly the card is removed from the lower window and displayed in the top window. Secondly any cards which are no longer needed to fulfil the SP's policy are greyed out in the lower windows. For example, if the SP's policy says that it needs a credit card from either Visa, Mastercard or Amex, and the user clicks on her Visa card, her other credit card icons will be greyed out in the lower windows. Until the combined set of selected cards match the full set of attribute types requested by the SP the "Use Selected Cards" button is disabled to prevent the user from incompletely authorising herself. Once the user has selected sufficient cards, the button is enabled and the LIS remembers this selection so that they can appear in the middle window the next time the same SP is contacted. *Because the LIS is in the cloud and not on the desktop, when the user moves from device to device she will not keep being told she has not sent cards previously to an SP when in fact she has,* as in the current CardSpace system.

The LS will query each of the chosen IdPs for the user's attributes (step 8.). All the chosen IdPs, including the self asserted IdP and the authenticating IdP, are contacted in the same way. The query comprises: an attribute query requesting the chosen subset of attributes required by the SP, a referral containing a PId encrypted to the recipient IdP, which points to the user's account at the IdP, and the original authentication token containing the random session ID. The recipient IdP uses the latter to determine whether it trusts the initial act of authentication by the authenticating IdP. If it does not, the recipient IdP returns an error to the LIS. If it does trust the authenticating IdP then it generates a claim containing the user's attributes encrypted to the SP (step 9). The user is identified in this assertion by the random session identifier contained in the authentication token. The LIS stores the returned claim until all the queried IdPs have replied.

Once all the attribute assertions have been collected by the LIS it generates a response to the original request made by the browser plug-in module. This response contains the authentication assertion and each of the encrypted attribute claims returned from the IdPs. When the browser receives the response it returns the enclosed claims to the SP (step 10). The SP receives a message containing a single authentication token and multiple attribute claims from multiple IdPs which all contain the same random session identifier. Since the SP trusts all the IdPs as being authoritative for their attributes, it can be assured that the same user possesses all of the returned attributes, and has been successfully authenticated to a particular level of assurance.

3. ACKNOWLEDGMENTS

The research leading to these results has received funding from the EC's FP7 programme under grant agreement n° 216287 (TAS³ - Trusted Architecture for Securely Shared Services).

4. REFERENCES

[1] David Chappell. "Introducing Windows CardSpace". MSDN. April 2006. Available from http://msdn.microsoft.com/en-us/library/aa480189.aspx

[2] OASIS. "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005

[3] William E. Burr, Donna F. Dodson, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus. "Electronic Authentication Guideline", NIST Special Publication NIST Special Publication 800-63-1, Feb 2008

[4] David W Chadwick, George Inman. "Attribute Aggregation in Federated Identity Management". IEEE Computer, May 2009, pp 46-53