Federated Identity Management for Protecting Users from ID Theft

Paul Madsen
NTT Advanced Technology
250 Cambridge Avenue, Suite 104, Palo Alto, CA 94306, USA
paulmadsen@ntt-at.com

Yuzo Koga
NTT Information Sharing Platform Laboratories
3-9-11 Midori-cho, Musashino-shi, Tokyo
180-8585, Japan
koga.yuzo@lab.ntt.co.jp

Kenji Takahashi
NTT Information Sharing Platform Laboratories
3-9-11 Midori-cho, Musashino-shi, Tokyo
180-8585, Japan
takahashi.kenji@lab.ntt.co.jp

ABSTRACT

Federated identity management is sometimes criticized as exacerbating the problem of online identity theft, based as it is on the idea of connecting together previously separate islands of identity information. This paper explores this conjecture, and argues that, while such linkages do undeniably increase the potential scope of a successful theft of identity information, this risk is more than offset by the much greater value federated identity, in combination with strong authentication, offers in preventing such theft in the first place.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; C.2.4 [**Computer-Communication Networks**]: Distributed Sysmtems—*Distributed Applications*

General Terms

Design, Security

Keywords

Federated Identity, Identity Theft, Phishing

1. INTRODUCTION

Federated identity is the dominant movement in identity management today. Federated identity refers to a model of distributed identity management in which one web site, in the interest of usability for users and efficiencies and economies for itself, decides to accept identity information and authentication operations maintained at another site. Federation refers to the establishment of business agreements, cryptographic trust, and user identifiers or attributes across security and policy domains to enable more seamless cross-domain business interactions.

The archetypical example of a federated application is web single sign-on (SSO), in which a user, after logging into one site, is able to access their resources held at other sites based on that initial authentication. The first site, rather than logging in the user directly (with the associated usability issues), relies on the second site to do so.

In addition to the improved online experience of SSO, federated identity management can provide reduced administrative costs of account maintenance for service providers, and a risk model more in line with service provider business models.

Federated identity management, in that it connects together previously isolated collections of identity information, might be perceived as only contributing to the identity theft problem - this by exacerbating the ramifications of any successful attack. The concern is that if one account is compromised, then any federated connections between that account and others will enable these other accounts to be compromised in a domino fashion. While this is a valid concern, federated identity, through its potential for enabling fewer and stronger authentication events, can actually hellp to minimize the risk of the initial theft. This paper will present a non-technical overview of the different ways by which federated identity management can actually help address certain aspects of the identity theft problem.

2. OVERVIEW OF ID THEFT ATTACKS

2.1 Phishing

Phishing refers to an identity theft attack in which an attacker lures a victim to a rogue website, typically by sending an email to the victim and encouraging them to click on a link. The victim, fooled by the apparent authenticity of both the email and the web site, may be convinced to provide identity information (e.g., account names, passwords, credit card info etc) to the rogue site.

Note: more evolved phishes do not even require a fake web site, the rogue site can simply proxy all interactions between the user and the authentic site in a Man In The Middle Attack.

Figure 1 illustrates the key steps in a phish.

DIM'05, November 11, 2005, Fairfax, Virginia, USA.

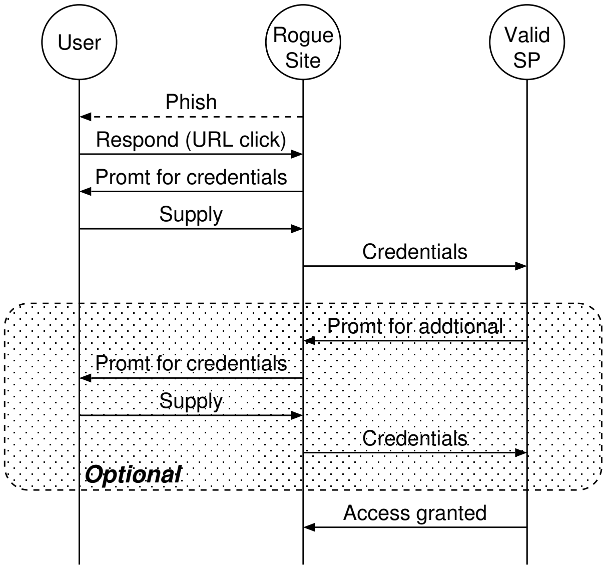


Figure 1: Key steps in a phish

2.2 Pharming

Pharming refers to an attacker acquiring the Domain Name for a site, and then redirecting legitimate traffic destined for that site to a rogue site impersonating the first. Once at the rogue site, the user may be fooled into providing personal identity information. Pharming can be viewed as a variant of a phish attack in which no email to the user prompting them to click on a link is necessary. Even if the user correctly enters a valid URL, the attacker can still redirect the user to the rogue web site.

Pharming attacks can be identified if the authentic site authenticates to the browser with SSL, as this should cause the browser to display a warning of a mismatch between the server certificate and the domain name. This however depends on the user not ignoring this warning.

2.3 Password Attacks

According to PricewaterhouseCoopers, the average user today has 40 personal and professional accounts requiring usernames and passwords. These passwords are typically weak and rarely changed. Even more seriously, many users reuse the same password across multiple sites. Consequently, if a rogue site is able to learn a user's password at one site, the chances are good that this password will also be useful at another. The criminals leverage the initial set of identity information to run credit checks and take other steps to ferret out all other accounts.

Critically, a rogue site may not even need to impersonate another valid site in order to get this (too often) 'global' password, all it need do is convince the user to create an account, which many users will be willing to do if they are offered some reward (e.g., free email or some promised coupon good at amazon.com).

3. WHAT IS FEDERATED IDENTITY MANAGEMENT

Federated identity management refers to a model of managing identities across policy and/or application domains in which the identity data is distributed but yet part of a virtual whole. In this model, different domains/sites choose to rely on identity data/operations that are held or occur elsewhere. In a sense, online federated identity can be compared to a passport of the physical world - countries choose to accept the passports (and the rigor of the issuance process) of other countries as proof of identity for that country's citizens (and thereby be freed from the burden of identifying any visitor itself.

Fundamentally, federated identity is portable identity - this portability dependent on syntax to describe the different aspects of online identity, protocols by which it can be moved around the network in a secure and privacy-respecting manner, and the business and legal frameworks under which business partners require to control risk.

4. FEDERATED IDENTITY ARCHITECTURE

In this section, we provide an overview of various federated identity management architectures.

4.1 OASIS Security Assertion Markup Language

The OASIS SSTC (Security Services Technical Committee) has defined SAML as a framework for expressing authentication and authorization information using XML syntax[8][9].

SAML defines an XML-based framework for communicating security and identity (e.g., authentication, entitlements, and attribute) information between computing entities. SAML promotes interoperability between disparate security systems, providing the framework for secure e-business transactions across company boundaries. By abstracting away from the particulars of different security infrastructures (e.g., PKI, Kerberos, LDAP, etc), SAML makes possible the dynamic integration necessary in today's constantly changing business environments.

The SSTC standardized SAML specifications for a) schema for the structure and content of assertions, b) protocols to exchange assertions, c) bindings over which the SAML protocols can be transported, and d) profiles that describe concrete sequence flows based on particular use-cases.

The Liberty Alliance's ID-FF architecture built heavily on earlier version of SAML. Recognizing the value of convergence, the Liberty Alliance contributed ID-FF as input to SAML 2.0, the most recent version of SAML[9].

4.2 Liberty Alliance

The Liberty Alliance architecture is depicted in Figure 2. The Liberty Alliance has defined technology specifications based on three frameworks, these are ID-FF (Identity Federation Framework), ID-WSF (Identity Web Services Framework), and ID-SIS (Identity Service Interface Specifications).

ID-FF defines a framework for federating identities and a mechanism for single sign-on in a federated manner. ID-WSF defines a framework for web services that allows providers to share users' identities in a permission-based manner (see section 4.2.2). ID-SIS defines service interfaces for each identity-based web services so that providers can exchange different aspects of identity (i.e., a user's profile) interoperably. The technical specifications for these three frameworks are publicly available at the Liberty Alliance website[1].

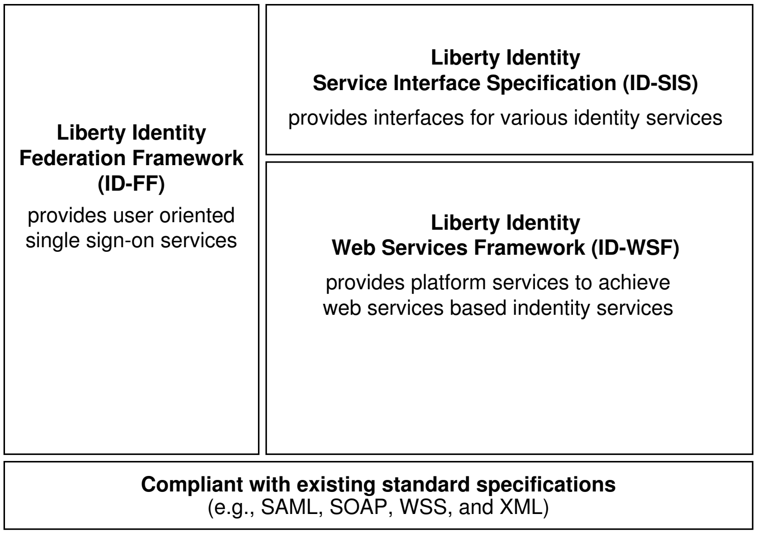

Liberty Identity
Federation Framework
(ID-FF)
provides user oriented
single sign-on services
Liberty Identity
Service Interface Specification (ID-SIS)
provides interfaces for various identity services
Liberty Identity
Web Services Framework (ID-WSF)
provides platform services to achieve
web services based indentity services
Compliant with existing standard specifications
(e.g., SAML, SOAP, WSS, and XML)

Figure 2: Overview of Liberty Alliance architecture

Note that the specifications for Liberty ID-FF are independent from those for Liberty ID-WSF. However, these can be closely related in cases of actual use-cases. For instance, an ID-WSF-based system can make use of the ID-FF framework for user authentication.

4.2.1 Identity Federation and Single Sign-On Mechanism

As described above, a user's accounts are distributed and maintained at each service site as deemed appropriate by that user. To federate these accounts whilst respecting user privacy, the identity provider and other providers establish a pseudorandom identifier (that is associated with a real name identifier at each site). The process of federating two local identities between providers is typically triggered by the user and with their consent - their involvement allows each provider to map the established pseudonym into their local account identifiers. This concept of identity federation is depicted in Figure 3.

When an authentication of a user is requested by a service providers, the identity provider authenticates that user appropriately and then issues an authentication assertion to that fact. If the identity provider has already authenticated a user, then it can just issue an assertion to that effect without necessarily requiring the user to present their credentials again.

Each service site validates the assertion issued from the identity provider, and determines whether or not it should be accepted. As the identity provider can issue multiple assertions to different service sites based on a single authentication action by the user, the user is able to sign-on to these other service sites without needing to be re-authenticated at each service site. A typical sequence flow for the single sign-on process is depicted in Figure 4 (details of the message flow between actors not shown).

4.2.2 Liberty ID Web Services Framework

Liberty Alliance defines the ID-WSF as a framework by which a user can share her/his personal information, main-

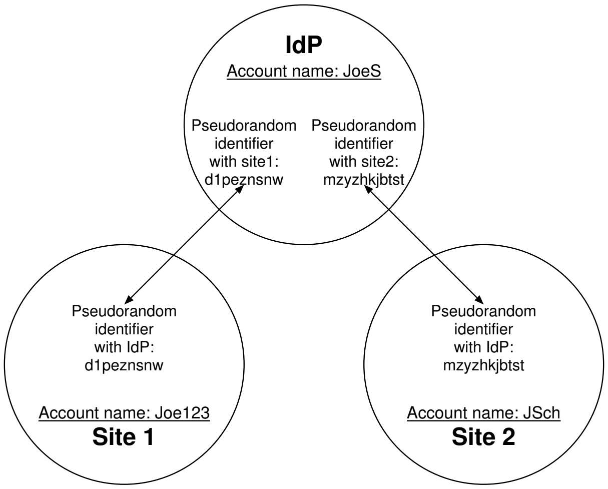

IdP
Account name: JoeS
Pseudorandom identifier with site1: d1peznsnw
Pseudorandom identifier with site2: mzyzhkjbtst
Pseudorandom identifier with IdP: d1peznsnw
Account name: Joe123
Site 1
Pseudorandom identifier with IdP: mzyzhkjbtst
Account name: JSch
Site 2

Figure 3: Identity federation

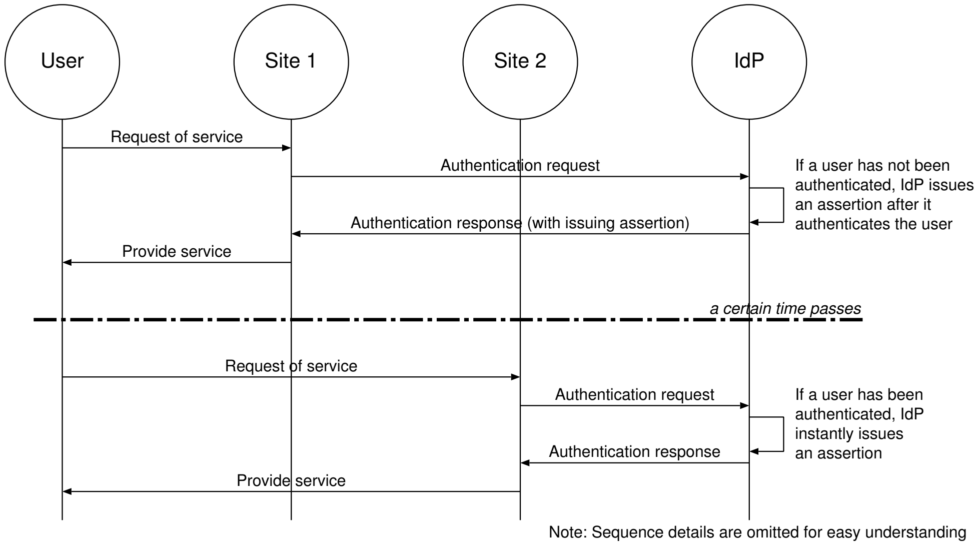

User
Site 1
Site 2
IdP
Request of service
Authentication request
If a user has not been authenticated, IdP issues an assertion after it authenticates the user
Authentication response (with issuing assertion)
Provide service
a certain time passes
Request of service
Authentication request
If a user has been authenticated, IdP instantly issues an assertion
Authentication response
Provide service
Note: Sequence details are omitted for easy understanding

Figure 4: Typical sequence flows for single sign-on processes

tained at certain service providers, with other service provider, based on the user's permission[5]. With this framework, once a user registers her/his personal information at a certain service provider, the information can be conveniently used at other service providers.

4.3 WS-Federation

WS-Federation [11] is a proposal from (primarily) Microsoft and IBM, part of their web services framework (often abbreviated as WS-*). WS-Federation describes how to manage and broker the trust relationships in a heterogeneous federated environment, including support for federated identities, sharing of attributes, and management of pseudonyms.

5. THE RISK

Federated SSO implies that, once authenticated to an identity provider, a user will be able to access resources held at federated service providers without additional log-ins. Of course, this also means that if an attacker is able to log-in as a particular user at an identity provider, they too will be able to access those federated service provider resources. At face value, it would seem that federated SSO only simplifies the job of the attacker, providing as it does a well known target (the identity provider) that, if successfully phished, provides a base of operations from which all the user's other resources at federated service providers can be stolen.

While this is true, we should recognize that the existing commonly occuring situation of passwords being reused across multiple sites presents a similar concern. Once one site is successfully phished/pharmed, the odds are not insignificant that those credentials will be useful at other sites. What's more, as there are no mechanisms by which sites could communicate the fact of one account being phished, the phisher will have time to perform its experiements with those credentials. So, in a sense, the accounts of many users at different providers are already linked - linked through the duplicate passwords those users use at the different sites. Today's reality (or at least a common scenario) is a chain of weak links, each one relatively easily broken and, once broken, providing an attacker the means to move up and down the chain.

In the federated world, there is also a chain linking together multiple sites, but with a important differences. Firstly, the chain can only be traversed from the strongest link to weaker links (i.e., there is no assumption of bilateral SSO)- breaking one of the weak links does not automatically give the ability to break either other comparably weak links nor the strongest link the identity provider). Secondly, if such a break is identified, federated identity standards provide mechanisms by which the damage can be contained through defederation.

6. FEDERATED IDENTITY MECHANISMS AGAINST IDENTITY THEFT

In this section, we discuss the potential advantages of federated identity management for combatting identity theft.

6.1 Login Frequency

Phishing depends on the rogue site being able to convince the victim to share identity information, often the account name and password for the site being impersonated. This task for the rogue site is greatly simplified by the general willingness of users to present such credentials to otherwise unknown sites. The current situation is that users are conditioned to expect to have to authenticate to the various sites they interact with, even if they feel that such authentication is not necessary for the task they wish to perform at that site.

Federated SSO will mean fewer authentication operations for users. A necessary side effect of this is that such operations will become less expected and more note worthy to the users. In a federated world, the prompt for credentials, which is today's default, will become a rarer occurrence - this relative infrequency will likely encourage users to question the validity of such prompts to a greater degree than currently.

In addition to becoming conditioned to authenticating fewer times, users will become conditioned to authenticating only to identity providers. Consequently, when prompted to log-in by what appears to be a service provider, the situation will be even more unusual and alarming.

Figure 5 illustrates how a user might be alerted to a phish solely through its unexpeced nature.

6.2 Login Attacks

Identity Federation and SSO, through reduced authentication operations, will make it practical for users to choose different (and stronger) passwords at their various identity providers. In addition to making brute force attacks on such passwords more difficult, any such 'strong' password, were it to be divulged, would not be immediately applicable at other providers because it would less likely to be reused there.

In addition, the login credentials that a user uses at the identity provider are never released to the service provider, only an assertion to their authentication status.

6.3 Service Authentication

Phishing and pharming both depend on a typical user's inability to adequately authenticate the site they are visiting. Simply by creating a reasonable visual imitation of a valid site, an attacker is able to convince many users of the supposed authenticity of the rogue site. While typical browsers support a variety of mechanisms (e.g. lock icon, address bar, warnings, etc) to help the user detect fraudulent sites, the burden remains on the user to interpret them.

Federated SSO acts to shift a significant portion of the burden of service provider authentication off the browser and user and on to the identity provider. This provider-provider authentication occurs through digital signatures and certificates so it is far less trivial for the rogue site to impersonate a valid site to the identity provider than is possible to the user. So, if the user were to not respond to a phish email by clicking on the presented link, but rather go to their identity provider and from there to the appropriate service provider, the attack would be circumvented.

Even if the user were to click on the phish link, but indicated that they would only authenticate at their identity provider, the rogue site would be unable to authenticate to the identity provider as the valid site and so the attack would fail as well.

6.4 Strong Authentication

Strong Authentication is typically used to refer to a security model in which something beyond account names and passwords are required in order to authenticate an entity to an acceptable level of confidence. Within this broad definition, the term strong authentication generally either refers to systems that depends on cryptography to allow an individual to prove they are who they claim to be or a layered authentication approach relying on two or more authenticators. Some systems demonstrate both aspects (e.g., use cryptography as part of a 2-factor authentication for instance).

Common to both interpretations is that strong authentication systems do not depend exclusively on the authenticators being shared across the network, either because cryptographic methods allow knowledge of the secret to be demonstrated without the secret itself, or because the form factor precludes such sharing. This can be contrasted with how passwords are used. By not depending on secrets to be shared across the network, strong authentication systems can be a significant defense against phish attacks because it prevents an attacker from being able to easily collect all the necessary credentials required to impersonate a user.

As an example, AOL's Passcode program distributes RSA SecurID devices to AOL members. The SecurID device generates and displays a unique six-digit numeric code every 60 seconds. To login to the AOL website, the user enters both their password and the SecurID code. Even if a user is fooled by a phish into providing their password and SecurID code, the SecurID code is time limited and so there is only a narrow window in which it could be used for another transaction at AOL.

It should be acknowledged that the AOL Passcode program (and similar OTP systems) does not prevent a man-in-the-middle (MITM) attack in which the attacker acts as a real-time proxy between the user and AOL, immediately presenting the password and SecurID Code to AOL as it receives them from the user. Nevertheless, such systems do significantly complicate the task for the attacker by limiting the time during which the stolen credentials will be accepted.

Another 2-factor approach to address phishing relies on multiple channels. For instance, a bank might deliver a secondary password to the user's cell phone via Simple Messaging Service (SMS). In order to login and to authorize financial transactions, the user must present both his password and the SMS password. Even if an attacker is able to phish the user's password for a particular site, that password on its own will be insufficient. Additionally, if the attacker tries a MITM attack, it would need to monitor both the browser and SMS channels in order to obtain all required credentials. One implication of this system is that the user must share their cell number with the bank, opening up the risk of receiving unwanted messages.

6.4.1 Strong Authentication and Federated SSO

Strictly speaking, strong authentication and federated identity are orthogonal, e.g., you can implement one without the other. However, when combined they provide a much more powerful defense against identity theft than either in isolation. Federated identity makes strong authentication more accessible/realistic for many sites by shifting the burden of the technology onto dedicated providers whose business model can more easily support the infrastructure costs.

Strong authentication, if implemented by each service provider, implies sending hardware tokens or key fobs to a large number of customers (even if not to the complete set), and so may be prohibitively expensive. Further, in the absence for interoperability standards between tokens and software, a symmetric hardware or software token is only capable of one provider relationship - the implication is that users will need to carry a token for each service provider (the so called 'token necklace' phenomena). Replacement of lost tokens adds to their cost. Many US banks tried large-scale deployments of multifactor strong authentication in the mid-1990s, but those initiatives were often abandoned, due to their cost and technical complexity.

Rather than each service providers having to implement strong authentication systems (with the likely implication of multiple tokens for the user to manage and carry), in a federated model a typical provider can 'outsource' the authentication to a dedicated 'strong authentication identity

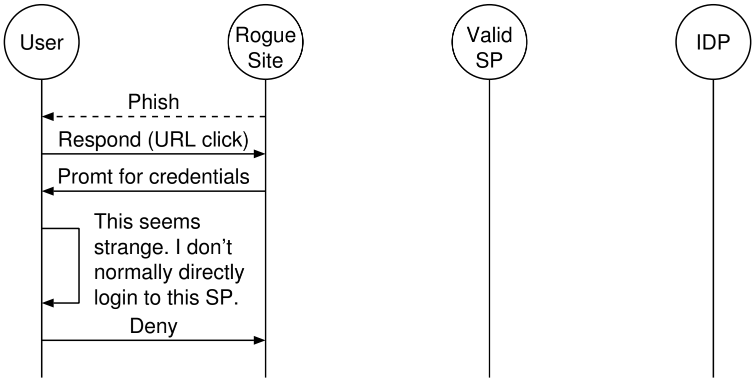


Figure 5: Passive federated defense for phishing

provider and then, through federated SSO, be able to benefit from the enhanced security the strong authentication provides.

Since the entire value of federated SSO is dependent on the ability of the service provider to trust the identities shared by the identity provider, strong authentication gives the added confidence necessary for high-value or sensitive transactions.

6.5 Opaque Identifier

The use of opaque identifiers by which different pairs of providers refer to users provides a partial measure of control over controlling the consequences of a successful identity theft. If a user's account at one provider is phished, identity theft or fraud. With federation, the identity provider and service provider together establish an opaque identifier(s) that are used to refer to a particular user in subsequent transactions. If

In addition to requiring that it be presented with a valid opaque identifier (i.e., one previously established with the identity provider purportedly presenting it) the service provider will base its trust in the identity provider's SSO assertion through signatures, certificate chains, validity intervals and other technical mechanisms. The credentials are transient and limited to a specific domain, and the opaque identifier is valid only between these two providers and therefore will not enable identity fraud to occur elsewhere if stolen.

Even if an opaque identifier were compromised, the partnering providers could easily substitute a new value with no negative impact to the user; indeed, users will almost certainly be oblivious to the actual value of the opaque identifiers used to refer to them[10].

6.6 User Interaction

The Liberty ID-WSF Interaction Service allows service providers, when deciding whether or not to release a user's personal information, to open up a channel to that user for confirmation. One of the profiles of the Interaction Service allows the service provider to invoke the Interaction Service provider in order to query a user for consent. The Interaction Service provider subsequently interacts with the user through an alternative channel (e.g., through SMS as described in section 6.4), in order to get consent for releasing information.

Consequently, the Interaction Service, by simplifying such two-channel interaction for service providers, can help protect users from a MITM identity attack. Figure 6 depicts how the Liberty ID-WSF Interaction Service can be applied to this multi channel model.

6.7 Authentication Management Processes

Federated identity enables an organization to balance authentication management between partners more equitably compared to alternatives such as remote accounts. For instance, if a certain employee's job responsibilities required that they be able to access resources at a partner site, that ability can be quickly revoked if and when that employee leaves the company.

Indeed, no such remote ”revocation” is necessary - the ex-employee loses his/her ability to access the partner site simply by having their local corporate account terminated.

6.8 Close and track breaches quickly and cleanly

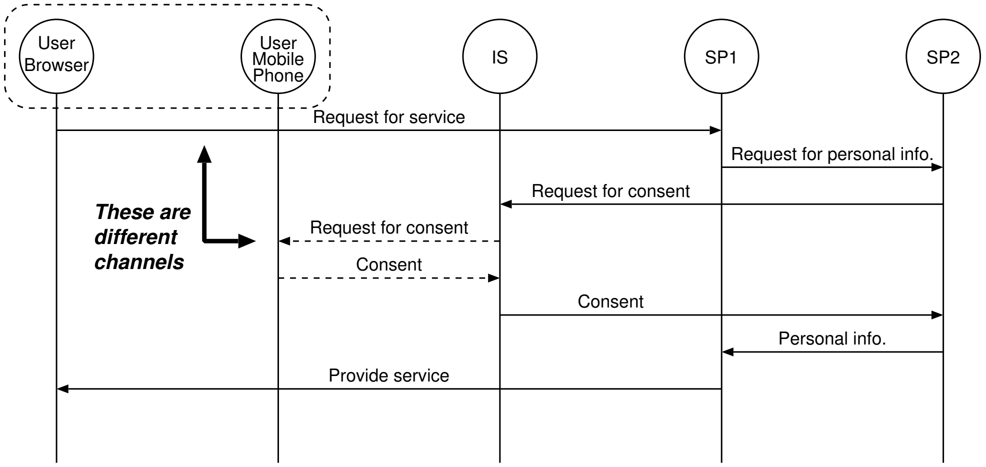
The fact that SSO assertions indicate the issuing identity provider allows the service provider to log this for potential future audits. If a user were to claim that activity conducted with a service provider was the result of identity theft/fraud originating elsewhere, then the service provider can easily determine if the entry point for this disputed activity in their domain was through a federated SSO with a particular identity provider or through an authentication performed locally at the service provider.

7. RELATED WORK

Various federated identity management applications and/or specifications have been analyzed for their security characteristics. For instance, both [13] and [14] examined Microsoft's Passport Network[12] and discovered vulnerabilities. Similar analysis of SAML 1.0 [15] resulted in the introduction in SAML 2.0 of mechanisms to address the identified vulnerabilities. In [16], WS-Federation was shown to provide authenticity and secure channel establishment in a realistic trust scenario.

8. CONCLUSIONS

The federated model for identity management is sometimes criticized because the “linking” of accounts that occurs is perceived to increases the risk of identity theft, or at least



SP1: a service provider that provides service using personal infomation at SP2.
SP2: a service provider that maintains user's personal information
IS: an Interaction Service provider

Figure 6: Multi channel model with Liberty ID-WSF Interaction Service

the ramifications of any breach. The reality is not so black-and-white. While it is undeniable that, if a user's account at an identity provider were to be successfully phished, the attacker would have opportunity to access other linked service providers, federation also makes practical many other mechanisms that serve to a) significantly complicate the initial theft (e.g. scalable strong-authentication), b) to identify and close a breach were it to occur (e.g. federation management protocols), and c) shift a significant portion of the burden of service provider authentication off the user on to identity providers.

9. REFERENCES

[1] Liberty Alliance Project. http://www.projectliberty.org/

[2] Organization for the Advancement of Structured Information Standards. http://www.oasis-open.org/

[3] S. Cantor and J. Kemp. Liberty ID-FF Protocols and Schema Specification. Version 1.2. Liberty Alliance Project. http://www.projectliberty.org/specs/

[4] S. Cantor and J. Kemp. Liberty ID-FF Bindings and Profiles Specification. Version 1.2. Liberty Alliance Project. http://www.projectliberty.org/specs/

[5] J. Tourzan and Y. Koga. Liberty ID-WSF Web Services Framework Overview. Version 1.1. Liberty Alliance Project. http://www.projectliberty.org/specs/

[6] J. Sergent Liberty ID-WSF Discovery Service Specification. Version 1.2, Liberty Alliance Project. http://www.projectliberty.org/specs/

[7] R. Aarts. Liberty ID-WSF Interaction Service Specification. Version 1.1. Liberty Alliance Project. http://www.projectliberty.org/specs/

[8] E. Maler, P. Mishra, and R. Philpott. Assertion and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. Version 1.1. OASIS Standards. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[9] S. Cantor, F. Hirsch, J. Kemp, R. Philpott, E. Maler, J. Hughes, J. Hodges, P. Mishra, and J. Moreh. Security Assertion Markup Language (SAML) V2.0. Version 2.0. OASIS Standards. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[10] W. Duserick. Whitepaper on Liberty Protocol and Identity Theft. Liberty Alliance Project. http://www.projectliberty.org/about/whitepapers.php

[11] S. Bajaj, G. Della-Libera, B. Dixon, M. Dusche, M. Hondo, M. Hur, C. Kaler, H. Lockhart, H. Maruyama, A. Nadalin, N. Nagaratnam, A. Nash, H. Prafullchandra, and J. Shewchuk, Web Services Federation Language (WS-Federation). Version 1.0. http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-federation.asp

[12] Microsoft Passport Network. http://www.passport.com/

[13] D. P. Kormann and A. D. Rubin. Risks of the Passport Single Signon Protocol. Computer Networks. Elsevier Science Press. Volume 33. pages 51-58. 2000.

[14] M. Slemko. Microsoft Passport to Trouble. http://alive.znep.com/ marcs/passport/. November 2001.

[15] T. Groß. Security Analysis of the SAML Single Sign-on Browser/Artifact Profile. 19th Annual Computer Security Applications Conference Proceedings. December 2003.

[16] T. Großand B. Pfitzmann. Proving a WS-Federation Passive Requestor Profile. 1st ACM Workshop on Secure Web Services (SWS). ACM Press. October 2004.