Regis University

ePublications at Regis University

Regis University Student Publications (comprehensive collection)

Regis University Student Publications

Fall 2011

An Analysis of User-Centric Identity Technology Trends, Openid's First Act

Peter Motykowski
Regis University

Follow this and additional works at: https://epublications.regis.edu/theses

 Part of the Computer Sciences Commons

Recommended Citation

Motykowski, Peter, "An Analysis of User-Centric Identity Technology Trends, Openid's First Act" (2011). *Regis University Student Publications (comprehensive collection)*. 628.
https://epublications.regis.edu/theses/628

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

AN ANALYSIS OF USER-CENTRIC IDENTITY TECHNOLOGY TRENDS, OPENID'S FIRST ACT

A THESIS

SUBMITTED ON 30 OF NOVEMBER, 2011

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

COMPUTER INFORMATION TECHNOLOGY

BY

PETER MOTYKOWSKI

APPROVALS

Christopher Garcia, Thesis Advisor

Shari Plantz-Masters

Ranked Faculty Name

Abstract

Identity technologies within Internet applications have evolved at an aggressive pace over the past decade. As a result, a variety of user-centric identity management technologies are available on the Internet today. The user-centric identity technology realm has become a fragmented ecosystem of standards, techniques, and technical approaches to identity management. A symptom of this fragmentation is the sluggish adoption of user-centric identity technologies by Internet users. A study titled, *An Analysis of User-Centric Identity Technology Trends, OpenID's First Act*, aims to reveal identity technology adoption patterns of users that engage in the use of Internet applications secured by an authentication credential. The study specifically focuses on Internet applications currently offering, or having at some point in time offered OpenID 1.x/2.0 (denoted OpenID hereafter), also known as OpenID's First Act. An extensive history of OpenID, from its inception as an emerging technology, to its declining rate of adoption as a standard for Internet single-sign-on, will be presented. A goal of this critical analysis is to reveal the shortcomings of OpenID that led to the discontinuation of the technology by prominent Internet applications. In support of this critical analysis, a survey is conducted which gauges the awareness of OpenID among casual Internet users. The results from this survey will be compared with observed trends among Internet applications to determine the contributing factors to OpenID's decline on the Internet and the subsequent efforts to reinvent the technology.

Acknowledgements

Without the support of those around me, the completion of this research would not have been possible. I offer sincere thanks to my lovely wife and children, who have exhibited great patience as I worked through the MSCIT degree program. Additional thanks to Christopher Garcia and Shari Plantz-Masters for guidance through the MSCIT degree program and thesis process.

Table of Contents

ABSTRACT ..... **I**

ACKNOWLEDGEMENTS ..... **II**

TABLE OF CONTENTS ..... **III**

LIST OF FIGURES ..... **V**

CHAPTER 1 – IDENTITY TECHNOLOGY OVERVIEW **1**

Internet Identity Technology History **1**

Username and Password Authentication **2**
Username and Password Reuse 3
Password Hygiene 4
Password Vaulting 5

Federated Identity **5**

Identity Provider **6**
Weak Authentication 7
Phishing 8

OpenID Authentication **9**
History of OpenID 12
Entrepreneurial Efforts 13
Janrain 13
Sxip Identity Corporation 14
OpenID Specification 14
OpenID Identity Providers 15
Advanced Authentication 17

CHAPTER 2 – REVIEW OF LITERATURE AND RESEARCH **18**

The Laws of Identity **18**
Control and Consent 18
Human Integration 19

A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On **19**

CHAPTER 3 – METHODOLOGY **21**

Sample Questionnaire **21**

CHAPTER 4 –RESULTS 23

Internet Presence 23
Search Engine Trending 23

Survey 24
Awareness Questions 24
Usage Questions 25

CHAPTER 5 – CONCLUSIONS 26

Internet Presence 26

User Awareness 26

Recent Deployments 27

Further Research 28

REFERENCES 29

APPENDIX A 32

Institutional Review Board Approval 32

List of Figures

Figure 1 - Example Internet application (http://linkedin.com) asking for email credentials. 4

Figure 2 - Example password management capability demonstrated via Firefox 5.x at http://stackoverflow.com. 5

Figure 3 - Example login component from http://stackoverflow.com featuring some OpenID capable identity providers with identity provider specific icons and arbitrary OpenID identifier specification 7

Figure 4 - Graphical Depiction of the OpenID Authentication Steps 10

Figure 5 - Example login component from http://sears.com featuring a constrained list of identity providers with site specific icons. 11

Figure 6 - Example password management capability demonstrated via Firefox 5.x. 20

Figure 7 - Search Engine Trending for term "OpenID" generated by http://www.google.com/trends. 23

Chapter 1 – Identity Technology Overview

With recent trends in identity related security threats on the Internet, users are being urged to employ extra measures to safeguard authentication credentials. Similarly, a subset of consumer-facing Internet applications in the United States have been mandated to implement sophisticated identity management techniques to aid in the protection of users (Costanzo, 2006). The rate in which user-centric identity technologies and techniques are adopted may largely influence the viability of the Internet as a safe place for users to conduct business or carry out social interaction (Cameron, 2005). Understanding the adoption of user-centric identity technologies is a goal of this study. To better comprehend the adoption of such technologies, an in-depth analysis of OpenID, and its adoption by Internet applications, will be performed to gain insight into the lifecycle of user-centric identity technologies.

For much of the Internet's history, it was sufficient to use rudimentary mechanisms, such as username and password combination as an authentication credential to govern access to web-based applications. As the sophistication of malicious Internet users grows, new techniques are required to ensure unauthorized access to Internet applications is made more challenging (Cameron, 2005). To frame the study, a brief history of Internet-based identity will be presented to demonstrate the sophistication necessary to protect access to Internet applications.

Internet Identity Technology History

The initial stages of the Internet had little need for the concept of identity and authentication. As entities of higher value began to join the worldwide network of computers, differentiating users of an Internet application was crucial to providing compelling features and securing private information. Unfortunately, identity was not included in any of the fundamental

protocol layers that comprise the Internet today (Cameron, 2005). Presently, username and password based authentication remains the predominant mode of authenticating a user of an Internet application. Steps have been taken to improve the sophistication of the username and password credential type. However, the credential type remains vulnerable to attack and has prompted computer security professions to seek more secure techniques for authenticating users (Costanzo, 2006). Additionally, the ubiquity of the username and password credential type has resulted in the phenomenon known as password fatigue. Password fatigue leads users to arrive at weak credential sets making it easier to memorize several username and password combinations for use at multiple Internet applications. This behavior ultimately reduces the security of the credential, therefore exposing the user to greater risk of credential theft (Josang, Al Zomai, & Suriadi, 2007).

OpenID entered the Internet application authentication landscape in 2005 (Fitzpatrick, 2005). This novel technology aims to reduce the number of username and password combinations a user must maintain for gaining access to Internet application by introducing many improvements to existing identity technologies, (Recordon & Reed, 2006).

Username and Password Authentication

The username and password credential type has been and remains the most ubiquitous form of authentication in use on the Internet. As a credential type, there is nothing particularly insecure about username and password. However, security issues arise around the proliferation of this credential type across multiple Internet entities. For example, the average Internet user maintains approximately twenty-five accounts across various Internet applications (Sun, Pospisil, Muslukhov, Dindar, Hawkey, & Beznosov, 2011). In most cases, each Internet application

requires a user to specify a set of credentials. When a user is faced with maintaining credentials for a multitude of Internet applications, the likelihood of poor credential management increases. Poor credential management manifests in many ways. When credentials are poorly managed, the likelihood of having credentials compromised is far greater. A closer look at poor credential management will help reveal ways that OpenID may strengthen the security of the username and password credential type.

Username and Password Reuse

When a user engages in the use of multiple Internet applications, the likelihood that username and password credentials will be reused is high. This convenient behavior allows a user visiting an Internet application quicker access via reused credentials. Reusing credentials is not an entirely poor practice if cryptographically strong passwords are being used. However, a major shortcoming of this behavior is the lack of centralized credential management. Should a reused credential become compromised, there is not an easy way for the user to change their password at all necessary Internet applications. As a result, there is a period of time a malicious user can use a compromised credential to access Internet applications. Additionally, the user is burdened with the need to update credentials at each Internet application to ensure unauthorized access will not continue.

While most OpenID implementations employ a username and password credential, the specification does not explicitly state what sort of authentication should be used (OpenID Authentication 2.0 - Final, 2007). Even when a username and password is in use via OpenID, considerable protection is afforded by the centralized nature of the credential storage. If the username and password credential of an OpenID account were compromised, the user could

change their password at the identity provider and the Internet applications associated with the OpenID will no longer accept the compromised credentials.

Password Hygiene

It's generally accepted that sharing beverage containers with others is considered poor personal health hygiene, sharing credentials is akin to this risky behavior. To safeguard username and password credentials, specifically the password portion, users are encouraged not to share their password and to use cryptographically complex characters when devising passwords. The behavior of sharing passwords is more common than one may think. For example, Figure 1 shows a sample Internet application that encourages users to provider their e-mail credentials so that contacts may be extracted for use in discovering fellow users.



Figure 1 - Example Internet application (http://linkedin.com) asking for email credentials.

Despite most Internet applications offering this feature state that credentials are not stored, it is generally considered poor practice to share credentials with anyone, even what may appear to be a trusted Internet application. This is considered poor practice because a malicious entity may construct a rouge Internet application that requests third party credentials with promise of a valuable service based on the obtained data. A naive user may be duped into providing their credentials and not recognize that the Internet application is indeed malicious

because of prior successful experiences with similar, but legitimate, Internet applications. Since it is challenging to distinguish a legitimate Internet application from a malicious one, engaging in credential sharing is not recommended. To facilitate a similar exchange of user information, an extension to the OpenID protocol defines a mechanism for attribute data exchange between Internet applications and identity providers (OpenID Attribute Exchange 1.0 - Final, 2007).

Password Vaulting

A common feature of popular web browsers is password vaulting. This feature offers storage of credentials for subsequent visits to respective Internet applications. While this feature seems reasonably secure, users expose themselves to significant risk by electing to vault credentials via any means. As demonstrated in Figure 2, the insertion of this capability into the interactions between a user and Internet application makes it a compelling alternative to more complex forms of identity management.

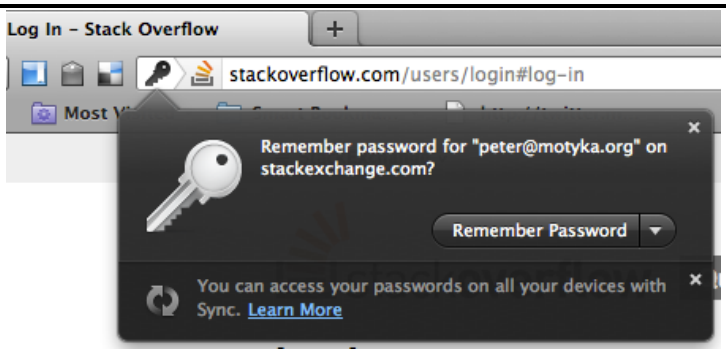


Figure 2 - Example password management capability demonstrated via Firefox 5.x at http://stackoverflow.com.

Federated Identity

The fundamentals underlying OpenID are not new to the identity management realm. OpenID employs a federated identity use case that allows a user to authenticate in one domain and assert their identity in another domain in a manner such that it is sufficient to satisfy the

target Internet applications authentication requirement. The action of engaging in the use of federated identity is called federated authentication or single sign-on. These same use cases are facilitated via other federated identity technologies such as Security Assertion Markup Language (SAML), WS-Federation, Shibboleth, and many other minor frameworks employing similar paradigms. OpenID builds upon its predecessors with the introduction of dynamic trust between identity providers and Internet applications via the establishment of associations (Recordon & Reed, 2006). The established association allows for subsequent messaging between the identity provider and Internet application with reduced overhead of renegotiating a shared secret. These features distinguish OpenID from other static trust federated identity technologies that usually require the exchange of cryptographic credentials via an out-of-band exchange.

Identity Provider

An identity provider is an entity on the Internet that challenges a user for some variant of authentication credential in order to validate a claimed identity. For example, Google serves as an identity provider by offering federated authentication via the OpenID protocol. As shown in Figure 3, Google is often available as an identity provider for Internet applications supporting federated authentication. In practice, Internet applications supporting OpenID tend to prefer specific prominent identity providers (Sun, Pospisil, Muslukhov, Dindar, Hawkey, & Beznosov, 2011). Although there are various reasons for this preference, a primary motivation is the lack of insight an Internet application has into the authentication event at the identity provider.

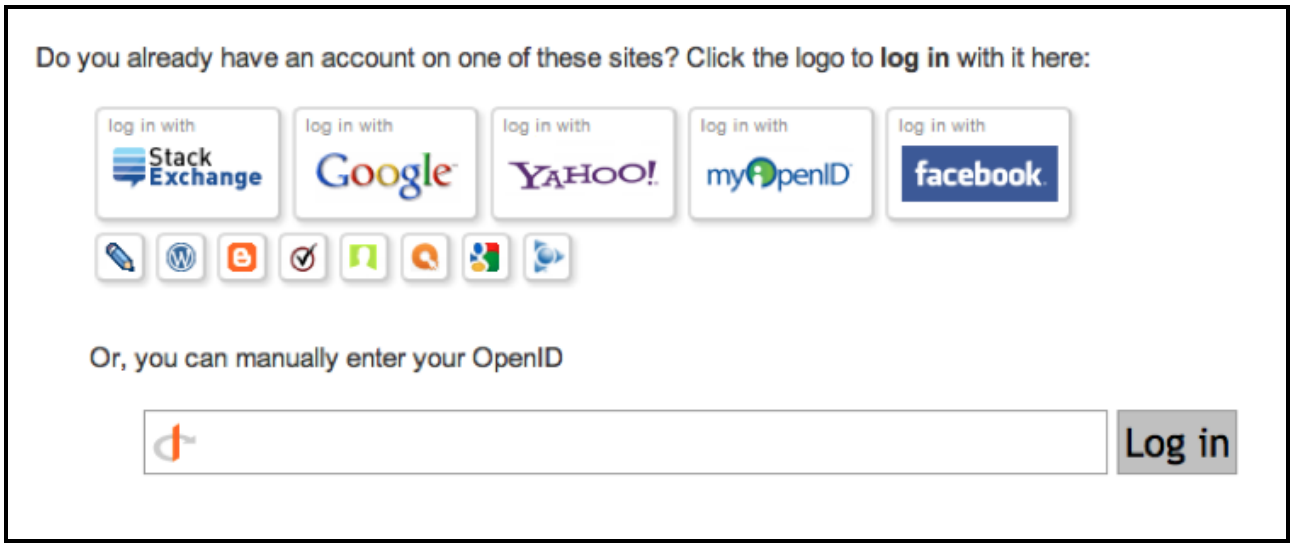


Figure 3 - Example login component from http://stackoverflow.com featuring some OpenID capable identity providers with identity provider specific icons and arbitrary OpenID identifier specification

To foster the truly open nature of OpenID, an Internet application should permit a user to specify their OpenID identifier. By specifying an OpenID identifier, the user is instructing the Internet application which identity provider should be used to carry out the OpenID transaction. Allowing the user to specify this critical piece of information to seed the authentication process is a defining characteristic that makes OpenID user-centric (Crompton, 2010). The user controls the initiation of the transaction and may even specify an identifier that leads the Internet application to use an identity provider under the administration of the user. Supporting arbitrary identity providers may be risky for Internet applications for the following reasons.

Weak Authentication

An integral piece of the authentication process is the event in which the identity provider collects the credential that is provided by the user. The event may result in the presentation of a username and password, the output of a cryptographic operation, a token, or any number of uniquely identifying pieces of data. Federated identity protocols often include a means to convey the type of credential used to authenticate a user. This valuable piece of data may be

passed to the partner Internet application to ensure the user was sufficiently challenged to verify their identity. For example, the SAML specification has been augmented with extensive metadata capabilities to express the type of authentication credential presented by the user. In order for interoperability to exist between federation partners, a set of Uniform Resource Identifiers have been established via the Organization for the Advancement of Structured Information Standards (OASIS) (Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005). By agreeing upon a limited set of credential type identifiers, Internet applications can be reasonably sure they are engaging in a secure identity transaction with an identity provider.

Phishing

Web-based federated authentication usually involves a web browser redirection from an Internet application to an identity provider for credential collection. This common pattern of credential collection has a significant shortcoming that is difficult to overcome. The exploitation occurs when the web browser is redirected an entity other than the identity provider intended to carry out the authentication event. This may occur as a deliberate act of a malicious Internet application or as the result of tampering with the communications between the Internet application and the web browser.

Phishing is a complex topic and serious problem for Internet application and identity providers wishing to engage in federated authentication. The OpenID Provider Authentication Policy Extension (PAPE) specification offers modes for an Internet application to request the identity provider use phishing resistant technologies. When directed to use phishing resistant technologies, an identity provider will ensure a Secure Hyper Text Transfer Protocol (HTTPS)

channel is used along with other techniques to reduce the risk of tampering with the communications between the identity provider, Internet application, and user.

OpenID Authentication

OpenID is fundamentally based on the action of verifying ownership of a resource. This resource is in the form of a publicly available Uniform Resource Locator (URL), specifically, an HTTP or HTTPS-based URL (OpenID Authentication 2.0 - Final, 2007). For example, consider Jane Doe who maintains the resource located at URL http://jane.doe.com. This URL is Jane's identifier and can be configured to facilitate OpenID authentication. The notion of an identifier is one of the major paradigm shifts introduced by OpenID. Internet users have long been comfortable with the notion of a username, and additionally the use of an email address as an identifier. Expressing identity as an identifier proved to be an abrasive user experience which led to the notion of an opaque identifier (Sun, Pospisil, Muslukhov, Dindar, Hawkey, & Beznosov, 2011). The opaque identifier technique is mostly employed by larger identity providers, Google for example, to avoid the need to initiate OpenID authentication with an unfamiliar URL-based identifier. As a result, many Internet applications list, usually using graphical icons, larger identity providers and users can initiate OpenID authentication by selecting their respective identity provider. This technique is at times referred to as directed identity, however, the OpenID specification titles the technique identifier selection (Norris, 2009). In Figure 4, a basic scenario using a user provided identifier will be presented to highlight the fundamental concepts of OpenID.

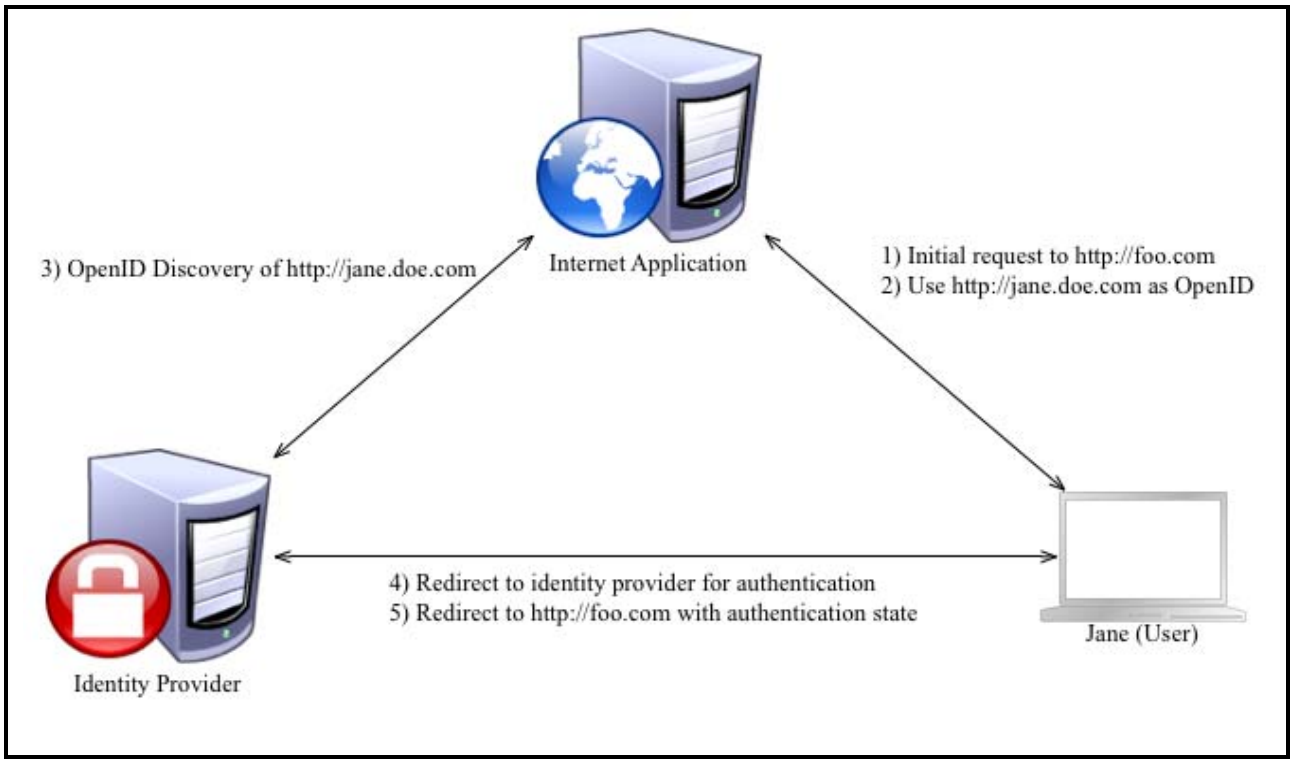


Figure 4 - Graphical Depiction of the OpenID Authentication Steps

1) Jane accesses an Internet application at URL http://foo.com.
2) Jane selects OpenID as her credential type and specifies http://jane.doe.com as her OpenID identifier.
3) The Internet application discovers the identity provider for identifier http://jane.doe.com and establishes a shared secret with the identity provider.
4) The Internet application redirects Jane to the identity provider discovered for her identifier and is challenged for a login credential.
5) Jane returns to http://foo.com via redirect by the identity provider with an indication of successful or failed authentication state.

A significant portion of the technical detail was omitted from these steps in attempt to make the interactions between actors clear. The important parts to take note of are, the Internet application allows Jane to specify her OpenID identifier and the Internet application

accepts the authentication state from the identity provider and permits Jane access. This flow demonstrates the truly open nature of OpenID in that an arbitrary identifier may be specified to access the Internet application. In practice, this aspect of OpenID has not seen widespread adoption and the permitted identity providers is typically a narrow list of prominent Internet identity providers, for example, Figure 5.

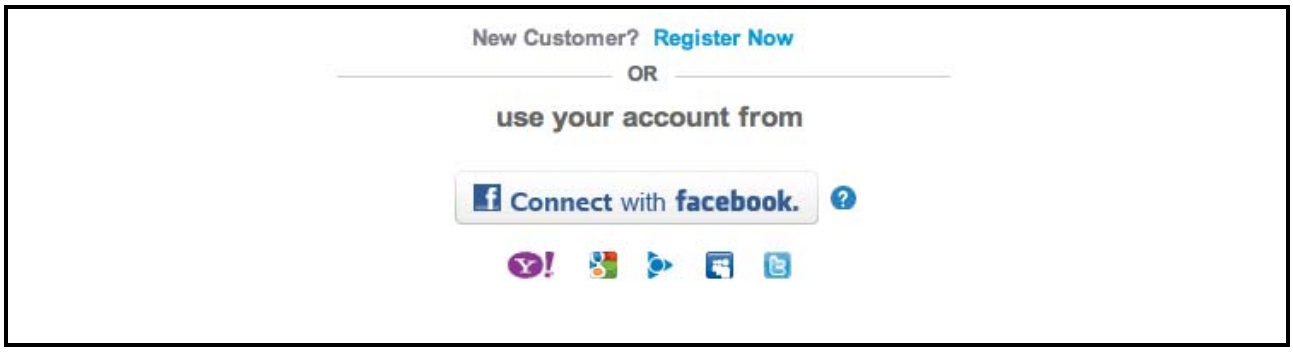


Figure 5 - Example login component from http://sears.com featuring a constrained list of identity providers with site specific icons.

The fact that most Internet applications employing OpenID have elected the practice of listing specific identity providers is a signal that OpenID's arbitrary identity provider notion may not be suitable for widespread deployment. Additional investigation will be performed to determine why this model is not appropriate for some Internet applications. While many aspects of OpenID have been found desirable by Internet applications seeking alternative authentication mechanisms, deficiencies in the technology have led to decommissioning of the technology by major Internet applications (Scribd, 2009) (37signals, 2011).

This study aims to answer the following questions with regards to OpenID's adoption and usage by Internet applications:

1) What risks do Internet applications face by permitting arbitrary OpenID identity providers to be used for authentication?

2) What issues resulted in Internet applications adopting the practice of listing specific identity providers for selection?
3) How does OpenID aid in the protection of users with respect to common credential theft attacks, such as Phishing?
4) How does OpenID increase the security of authentication above what is provided by a username and password credential?

History of OpenID

The earliest innovations leading to the creation of OpenID are those of Livejournal.com founder, Brad Fitzpatrick. During the year 2004, Fitzpatrick began working with Live Journal, a journaling Internet application popularized as a means for self-published content. Fitzpatrick envisioned an identity system which eased the user experience of publishing comments on journal entries on LiveJournal.com. Initially, the project was named YADIS, which expands to "Yet Another Distributed Identity System". The nature of this moniker suggests that the notion of distributed identity was not new and Fitzpatrick was making another attempt to solve the Internet authentication problem (Kim, 2005).

LiveJournal.com, being based on an openly distributed content management system (CMS) code base, gained interest in OpenID by making the feature available in June 2005. Shortly after, other Internet applications based on the same CMS became OpenID capable by updating to the latest Live Journal code base (Fitzpatrick, 2005). Initially, the protocol was promoted for low value transactions, specifically, leaving comments on journal entries. Shortly after being made available, it became clear the protocol was robust enough for higher value Internet application authentication. Other prominent Internet entities took notice of OpenID and joined forces in evangelizing the technology, along with engineering support for the protocol in

their Internet applications. OpenID continued to take the Internet by storm with the establishment of start-up companies aiming to capitalize on value added services around OpenID adoption and deployment.

Entrepreneurial Efforts

Like most new technologies, OpenID's popularity inspired entrepreneurs to create new businesses that strived to deliver value added features and services to users. Additionally, these fledgling companies participate extensively in the drafting of specification documents and the governance processes surrounding OpenID protocol definition. Two companies that made significant contributions to the OpenID community are Janrain and Sxip. A closer look into the contributions of each entity will highlight the unique role such actors play in new technology development.

Janrain

Janrain was established in mid-2006 and initially focused on Internet application integration componentry for OpenID. These components became widely adopted by Internet applications and remain actively supported by either Janrain or teams of Open Source developers. The development of integration componentry has been a successful strategy for Janrain. Their portfolio of products and services is predominately oriented towards this sort of offering and primarily targets user-centric identity technology, such as OpenID. An area of focus of Janrain has been the enhancement of user experience of user-centric technologies. Products such as Janrain Engage go to considerable lengths to provide an effective user interface for interacting with specific identity providers along with a means for providing an arbitrary OpenID identifier.

Janrain continues to be successful with its ventures around user-centric identity technologies and remains a respected member of many of the communities responsible for technology specification. Their continued success is evident via the claim of 350,000 active deployments of Janrain products and services along with the securing of additional capital further grow the company (Janrain, 2011).

Sxip Identity Corporation

Sxip Identity Corporation was started by identity technologist Dick Hardt. Hardt gained the attention of the identity community with his iconic Identity 2.0 presentation at the 2005 O'Reilly Open Source Convention (OSCON). Hardt tried to manifest the ideas expressed in the Identity 2.0 presentation via Sxip's products and services. One of Sxip's most successful products was Sxipper, a browser plug-in which eased the usage of user-centric identity technologies. Unfortunately, Sxip and their products and services did not succeed as well as needed to sustain the company. Sxip was dismantled via various corporate dealings with the Sxipper product surviving as its own company for a few more years. Hardt remains an active technologist in the identity community and recently facilitated a session titled Decline of User-Centric Identity at the 2011 Internet Identity Workshop (IIW). Hardt asserts that recent trends in identity technology are straying from the user-centric architectures of protocols like OpenID. Hardt's influence on OpenID may be dwindling as he is no longer serving at the board level of the OpenID Foundation.

OpenID Specification

As OpenID gained interest by technologists and Internet entities, the need for more formal specification of protocol became necessary. The specification process is primarily managed via the OpenID specification electronic mailing list. The initial finalized release of the

OpenID specification is version 1.1 and was published in May 2006. This specification formalized much of the OpenID protocol which was already deployed widely by Live Journal and affiliated Internet applications. Specification work continued and culminated with the publishing of the OpenID 2.0 specification in December 2007. The subsequent release of the specification addressed various security issues, interoperability challenges, and generally improved the protocol with additional features.

Somewhat tangential to the OpenID specification effort is the establishment of the OpenID Foundation. This organization aims to evangelize the technology, sponsor interoperability exercises, and serve as a central information repository for topics related to OpenID. Of particular significance to the OpenID community, the foundation manages the intellectual property and contribution agreements. In order for an individual or Internet entity to participate in the OpenID specification process, an agreement must be submitted that surrenders rights of contributions to the body of work. This exercise is vital to the health of a community defined specification to ensure no person or entity can claim ownership of OpenID or related technologies.

OpenID Identity Providers

The open nature of OpenID stems from the user's provided identifier dictating which identity provider will be used for authentication. Internet applications accepting OpenID may be uncomfortable with a fully open mode of operation due to the risk involved in accepting users from arbitrary identity providers. For example, identity provider implementations exist that do not require a username or password and use an anonymous randomly generated identifier. Such services compromise the integrity of the OpenID ecosystem as the Internet application cannot be certain a user has been sufficiently challenged for credentials. While extensions to OpenID, such

as OpenID Provider Authentication Policy Extension (PAPE), have been proposed, most Internet applications have chosen a defensive posture and restrict OpenID authentication to large trustworthy providers.

Provider Authentication Policy Extension (PAPE)

The OpenID community recognized the necessity for Internet applications to verify how users authenticate at an identity provider. However, this capability is not part of the core OpenID protocol specification. To address this deficiency, a subsequent specification was drafted titled OpenID Provider Authentication Policy Extension (PAPE). This specification defines a mechanism in which Internet applications may include additional information conveying which authentication credential types are considered sufficient for authentication. Unfortunately, not all OpenID identity providers offer PAPE capabilities and Internet applications need to account for this if interoperating with arbitrary identity providers. The PAPE capability is best suited for Internet applications that are constrained to a fixed set of identity providers that offer PAPE such that OpenID protocol messaging can be enhanced with enhanced authentication metadata.

Open Identity Exchange (OIX)

The Open Identity Exchange (OIX) is an organization which maintains a registry of identity providers that have completed a rigorous certification processes. The OIX registry contains a short list of identity providers who offer profiled OpenID features and extensions that have been deemed as meeting a specific level of assurance (LOA). Based on the security features of the identity provider, higher LOA profiles may be available to further protect the identity transaction. The efforts of the OIX provide a valuable service to a user-centric identity ecosystem that may at times seem completely unregulated. By engaging an identity provider

from the OIX registry, an Internet application can be reasonably certain the user-centric identity technology in use has been implemented properly.

Advanced Authentication

While some identity providers intentionally try to degrade the security of the OpenID ecosystem, many others strengthen the user's security environment with the use of strong authentication credentials. While username and password remain the predominant means for authentication for Internet applications, some OpenID identity providers are aiming to improve authentication security for users that select their identity provider. Clavid AG is one such identity provider that allows users to use strong authentication mechanisms, such as One Time Password (OTP), Client Certificate, and biometric technologies. Such identity providers help realize the true potential of OpenID. In such a scenario, Internet applications could reduce the level of effort expended implementing authentication technologies and simply use OpenID with the necessary PAPE extensions to describe identity provider authentication strength. It is the realization of this scenario that may revive OpenID in subsequent version specifications and reduce the need for Internet applications to restrict permitted identity providers.

Chapter 2 – Review of Literature and Research

The Laws of Identity

The Laws of Identity is a seminal work by technology thought leader Kim Cameron that has influenced many of the identity protocols used on the Internet today. Cameron painstakingly details the evolution of Internet identity and the problems resulting from often short sighted solutions. The seven points outlined by Cameron have indeed become the laws of identity and are often referenced in scholarly research publications when evaluating emerging identity technologies. Cameron asserts that technologies not adhering to all seven laws will ultimately fail as users disband usage when risks become evident. The specific laws that stand out as essential qualities of viable identity are User Control and Consent and Human Integration. These laws are of particular interest when considering OpenID and its short comings as an identity technology.

Control and Consent

Control and Consent is the first law of identity as proposed by Cameron. At the core of the Control and Consent law is the user of the identity system. The law lays the foundation of user-centric principles being paramount to the success of an identity technology. While OpenID goes to great lengths to abide by the Control and Consent law, it falls short with regards to protecting the user from deception. The failure to natively address the risk of a user being redirected to an entity other than the intended identity provider is a violation of Control and Consent that ultimately leaves the user vulnerable to credential theft. Although the PAPE extension to OpenID attempts to address this issue, being an optional enhancement to the authentication process does not provide the user with consistent protection to consider the risk fully mitigated.

Human Integration

The Human Integration law addresses the importance of user experience in the success of an identity technology. By far, much of the criticism OpenID receives is related to the user experience making for an unpleasant and confusing authentication event. First, and foremost, the use of a URL as a user identifier largely confuses users. This foreign expression of identity leaves users unsure how to engage an Internet application. Although this usability deficiency has been addressed with icons leading users to specific identity providers, this user interface paradigm does not scale well. It Internet applications were to simply keep adding icons for specific identity providers, users would be faced with far too many options to choose from, resulting in a cumbersome process locating their identity provider.

A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On

This proceeding from a prominent identity conference approaches the Internet federated authentication (single sign-on) problem from several interesting directions. The authors assert the single sign-on use case may be compelling from an academic standpoint, however, the value propositions for users, identity providers, and target Internet applications are insufficient. The assertion made about users is very interesting and makes several valid points about the current environment in which users operate within to access Internet applications. Many users access Internet applications using a desktop computer featuring an operating system with web browser installed. Most modern web browsers feature some sort of embedded password vaulting capability.

The authors make a valid point when suggesting that embedded password vaulting tools are sufficient for most users. These tools recognize when a user is interacting with an Internet

application that requires authentication and offers to cache the credential for subsequent visits. While the security of these tools is questionable, users often find the capability's convenience outweighs the risks of storing passwords on their computer for later usage. Stored passwords may be encrypted by some tools, however, popular embedded web browser password vaults allow for the recovery of passwords with relative ease. Figure 6 provides a view of a popular embedded web browser password vault that offers viewing of passwords in clear text.



Figure 6 - Example password management capability demonstrated via Firefox 5.x.

Chapter 3 – Methodology

The qualitative research study has been performed via an extensive literature review of existing publications relevant to the user-centric identity subject. Additionally, a survey was conducted to assess the level of OpenID exposure amongst a carefully selected set of Internet users. The results of these exercises will be analyzed to arrive at a conclusion that satisfactory meets the objectives of the study stated in the abstract.

The participants of this study were provided an anonymous Internet-based survey containing a variety of multiple-choice and rating scale questions. The questions are intended to gauge the participants' level of awareness and comfort using OpenID technology. The survey will be administered using the SurveyMonkey online survey software & questionnaire tool. The recipients of this survey will be derived from personal contacts of the author of this study, and via solicitation of participants via public Internet forums. A minimum of 25 completed questionnaires will be analyzed for this study.

Sample Questionnaire

1) Have you heard of OpenID technology?
    a. Yes, very aware of its existence and purpose
    b. Yes, heard of it but not really sure what it has to offer
    c. Yes, but I thought it was called OpenID Connect
    d. No

2) What is your level of comfort with OpenID technology?
    a. Expert
    b. Knowledgeable
    c. Novice
    d. Never heard of it or used it

3) Do you have an account with an OpenID provider?
    a. Yes, with many OpenID providers
    b. Yes, with only one provider
    c. No
    d. I don't know

4) How often do you use OpenID?
    a. Frequently, used to access most Internet applications
    b. Often, used to access a few Internet applications
    c. Seldom, used to access one Internet application
    d. Never

5) When creating a new account/or logging into an existing account, do you use features such as "Login using Google", or "Login using Facebook".
    a. Yes, always
    b. Yes, sometimes
    c. No
    d. I don't know

6) Are you aware that the "Login using Google" feature offered by some Internet applications is currently implemented using OpenID?
    a. Yes
    b. I suspected that may be the case
    c. No

7) Rate the overall user experience offered by OpenID technology using the scale below:
    a. Satisfied
    b. It gets the job done but could use improvement
    c. Unusable
    d. Never used it

Chapter 4 –Results

Internet Presence

One of the ways the decline of OpenID manifests itself is the decreasing presence in technology media and the marketing the technology is receiving. This decline is demonstrated via the presentation a metric called search engine trending.

Search Engine Trending

A technique used to gauge the presence of a topic on the Internet is search engine trending. This technique reveals how often a term is being searched for and visualizations are rendered to show the overall progression of a trending topic on the Internet. The following figure depicts the search term "OpenID" and its corresponding trend data for the Google Search Engine.

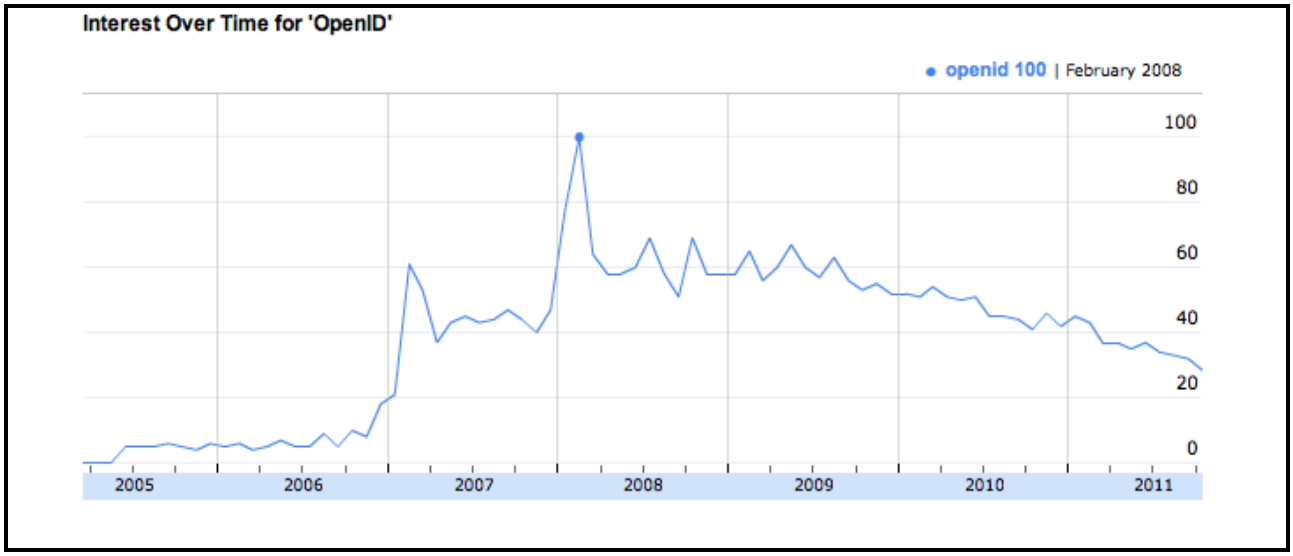


Figure 7 - Search Engine Trending for term "OpenID" generated by http://www.google.com/trends.

Figure 7 shows a distinct rise in search engine activity around February 2007 and another significant spike in activity February 2008. The first spike in activity in February 2007 coincides with the announcement made by America OnLine (AOL) which stated that the Internet entity

supports OpenID. This support is limited to the identity provider role and applicable to all user accounts within the AOL.com domain. The announcement boasted that effectively 63 million OpenID-enabled accounts we're ready to be used. This announcement generated significant activity on the Internet in the form of both positive and negative feedback.

The second spike in activity seen in February 2008 coincides with the announcement of several large corporate Internet entities joining the OpenID board. The notable list of corporations, Google, Yahoo!, IBM, Microsoft, and VeriSign attracted significant attention towards OpenID as is evident by Figure 7. The act of joining the board suggests that these corporate entities were dedicated to seeing OpenID success and were going to advocate for its adoption within their Internet applications.

Survey

The intention of the conducted survey is to measure casual internet users' awareness of OpenID identity technology. The participants of this survey are individuals with basic skills using Internet applications, however, are not information technology experts or professionals. The results of the survey indicate a general ignorance of OpenID identity technology and its related use cases. These results suggest that attempts to market and evangelize OpenID to Internet users were largely unsuccessful. Furthermore, like other identity technologies, OpenID is best left as an infrastructure technology and further attempts to make casual users aware of its usage only detracts from the user experience.

Awareness Questions

The first three questions of the survey aimed to gauge the awareness of OpenID technology. 90% of respondents reported they either never heard of OpenID or were vaguely aware of its existence and purpose. Furthermore, 90% of respondents stated that they do not

have an account with an OpenID identity provider or were unsure if they had an account. These results are a clear indication that OpenID technology has not made a major impact amongst casual Internet application users. Considering that the majority of casual Internet users have accounts with major Internet entities offering OpenID, such as Google, Yahoo!, and AOL, users are seemingly unaware that OpenID authentication is available for their usage.

Usage Questions

The last four questions of the survey aimed to gauge usage information of OpenID amongst casual Internet users. For example, question five inquired about usage of major Internet entities offering OpenID, such as Google, when authenticating to other Internet applications. Thirty percent of respondents acknowledged engaging in this use case. This response was quite divergent from the other questions which asked outright about OpenID usage. The overwhelming majority of respondents reported never using OpenID. This contradictory data demonstrates that casual Internet users are simply unaware that they are using OpenID technology to carry out some of their Internet application authentication events.

Chapter 5 – Conclusions

A goal of this critical analysis is to reveal the shortcomings of OpenID that led to the discontinuation of the technology by prominent Internet applications. Through the analysis of peer reviewed documentation and data collection, it has been concluded that the combination of awkward user experience, poor identity provider security, and lack of OpenID user awareness lead to OpenID's declining rate of adoption as a standard for Internet single-sign-on. As the OpenID Foundation currently works to deliver a new version of the protocol, these issues will hopefully be addressed and the user-centric identity technology will be reintroduced to Internet users and applications with more compelling features.

Internet Presence

As demonstrated by the Figure 7 search engine trending data, OpenID has seen a steady decline in Internet search activity, specifically via the Google Search Engine. While this trend may continue, there is a distinct chance that trending data may reverse as activity within the OpenID community increases around the specification of the next version of the protocol. While this reversal of activity may suggest a renewed interest in OpenID's First Act, instead it will reflect interest in the workings of the OpenID Foundation towards subsequent protocol specification release.

User Awareness

The survey conducted yielded results suggesting casual Internet users are largely unaware of OpenID as a technology, although they may be using it to carry out authentication events with

Internet applications. This phenomenon suggests that casual Internet users need not be aware of the underlying authentication protocols employed by Internet applications.

OpenID's First Act involved considerable marketing targeted at users. User were encouraged to learn about the technology and then steered towards identity providers and Internet applications which employed the technology so they could begin using it. It can be concluded that this marketing approach was largely ineffective. Most Internet application users are generally uninterested in the technologies being used to facilitate authentication and are more concerned with a pleasant user experience. If an identity technology is trying to draw attention to it simply to gain awareness, the user is being distracted from their primary goal of Internet application usage. Users want functional Internet applications and have little tolerance for unnecessary steps in Internet application usage (Sun, Pospisil, Muslukhov, Dindar, Hawkey, & Beznosov, 2011).

Recent Deployments

Despite what seems like a decline in the adoption and usage of OpenID, a significant new deployment has recently been publicized by a major Internet entity. PayPal, a leading ecommerce transaction facilitator, announced PayPal Access, which is based on OpenID 2.0. This deployment suggests that OpenID may remain viable for the identifier selection scenario in which authentication is constrained to a single or finite list of identity providers. To properly measure the success of this specific deployment, further research may be conducted to determine how many Internet applications permit the PayPal Access technology to be used as an authentication option. This specific deployment addresses the assertion that no value propositions exist to drive Internet application and user adoption of user-centric identity

technologies. PayPal, being a financial transaction facilitator, introduces a strong motivator by easing the authentication process at Internet applications and readying users to complete an ecommerce transaction without secondary authentication.

Further Research

OpenID's First Act concluded with mixed views of the overall protocol's success among identity technologists. While several large prominent deployments of OpenID remain on the Internet today, chances are these deployments will migrate to the next version of OpenID as it becomes available. Initial specification drafts reveal the next version of OpenID being a complete divergence from the architectural underpinnings of OpenID's First Act. Will major deployments of OpenID remain on the current architecture as it seems to meet their needs at the moment? Revisiting this topic after the next version of OpenID specification is released would further aid in determining if OpenID's First Act was a success, failure, or neither. It just may be that OpenID's First Act was a necessary evolutionary step along the lifecycle of user-centric identity protocol development.

References

Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. (2005, March 15). Retrieved 19 2011, 08, from http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

OpenID Attribute Exchange 1.0 - Final. (2007, December 05). Retrieved 09 01, 2011, from http://openid.net/specs/openid-attribute-exchange-1_0.html

OpenID Authentication 2.0 - Final. (2007, December 5). Retrieved 01 2011, 10, from http://openid.net/specs/openid-authentication-2_0.html

37signals. (2011, January 25). *We'll be retiring our support of OpenID on May 1*. Retrieved 05 12, 2011, from 37signals Product Blog: http://productblog.37signals.com/products/2011/01/well-be-retiring-our-support-of-openid-on-may-1.html

Cameron, K. (2005, May). *The Laws of Identity.* Retrieved 07 01, 2011, from Microsoft Developer Network: http://msdn.microsoft.com/en-us/library/ms996456.aspx

Costanzo, C. (2006, March). out with the old, in with the new: Evolving Trends in Information Authentication. *Community Banker*, pp. 48-51.

Crompton, M. (2010). User-centric identity management: An oxymoron or the key to getting identity management right? *Information Polity*, 291-297. doi:10.3233/IP20100193

Fitzpatrick, B. (2005, 06 27). *OpenID support*. Retrieved 09 21, 2011, from Livejournal: http://news.livejournal.com/86532.html?thread=25389316

Janrain. (2011, 08 03). *Janrain Raises $15.5 Million Investment Led By Premier SaaS Venture Firm Emergence Capital Partners.* Retrieved 11 04, 2011, from Janrain Web Site:

http://www.janrain.com/press-releases/janrain-raises-15-million-investment-led-premier-saas-venture-firm-emergence-capital

Jøsang, A., Zomai, M. A., & Suriadi, S. (2007). Usability and Privacy in Identity Management Architectures. *Australasian Information Security Workshop.* Ballarat: Australian Computer Socieity, Inc.

Kim, E. E. (2005, May 17). *yet another distributed identity system (yadis).* Retrieved 10 04, 2011, from Blog: http://eekim.com/blog/2005/05/yet-another-distributed-identity-system-yadis/

Norris, W. (2009, July 31). *Directed Identity vs Identifier Select*. Retrieved 09 17, 2011, from http://willnorris.com/2009/07/openid-directed-identity-identifier-select

Recordon, D., & Reed, D. (2006). OpenID 2.0: A Platform for User-Centric Identity Management. *Proceedings of the second ACM workshop on Digital identity management.* Alexandria: ACM. doi:10.1145/1179529.1179532

Scribd. (2009, March 1). *Does Scribd support OpenID?* Retrieved 8 14, 2011, from Scribd Support Desk: http://support.scribd.com/entries/25547-does-scribd-support-openid

Sun, S.-T., Boshmaf, Y., Hawkey, K., & Beznosov, K. (2010). A billion keys, but few locks: the crisis of web single sign-on. *Proceedings of the 2010 workshop on New security paradigms* (pp. 61-72). New York: ACM. doi:10.1145/1900546.1900556

Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). OpenID-Enabled Browser: Towards Usable and Secure Web Single Sign-On. *ACM CHI Conference on Human Factors in Computing Systems.* Vancouver: ACM. doi:10.1145/1979742.1979763

X.commerce. (2011, 10 12). *PayPal and X.commerce Launch PayPal Access.* Retrieved 10 15, 2011, from Business Wire: http://www.businesswire.com/news/home/20111012006418/en/PayPal-X.commerce-Launch-PayPal-Access

Appendix A

Institutional Review Board Approval

REGIS UNIVERSITY

Academic Affairs
Academic Grants

3333 Regis Boulevard, H-4
Denver, Colorado 80221-1099

303-458-4206
303-964-3647 FAX
www.regis.edu

IRB – REGIS UNIVERSITY

October 25, 2011

Peter Motykowski
1158 Eudora Street
Denver, CO 80220

RE: IRB #: 11-308

Dear Peter:

Your application to the Regis IRB for your project "An Analysis of User-Centric Identity Technology Trends, OpenID's First Act" was approved as exempt on October 25, 2011.

Supporting reference information from the chair: "…approved as an exempt study under 45CFR46.101(b)(2) (survey research). A consent form is not required for exempt studies, but a statement of consent on the opening page of the survey is suggested.

The designation of "exempt," means no further IRB review of this project, as it is currently designed, is needed.

If changes are made in the research plan that significantly alter the involvement of human subjects from that which was approved in the named application, the new research plan must be resubmitted to the Regis IRB for approval.

Sincerely,

Daniel Roysden, Ph.D.
Chair, Institutional Review Board

cc: Christopher Garcia

A JESUIT UNIVERSITY