HÖGSKOLAN SKÖVDE

Institutionen för kommunikation och information

Comparison of Liberty Alliance and OpenID regarding their ability to protect the confidentiality, integrity and availability of the users' information

A study based on the analysis of resistance to common attacks

Jaqueline de Souza

Bachelor's Thesis in Computer Science
15 ECTS credits, C-Level, Year 2010

Comparison of Liberty Alliance and OpenID regarding their ability to protect the confidentiality, integrity and availability of the users' information

A study based on the analysis of resistance to common attacks

Submitted by Jaqueline de Souza to the University of Skövde as a final year project towards a degree in B.Sc. in the School of Humanities and Informatics. The project has been supervised by Jakob Ahlin.

Friday, August, 20 2010

I hereby certify that all material in this final year project which is not my own work has been identified and that no work is included for which a degree has already been conferred on me.

Signature:

Abstract

It is essential to solve the problem due to password fatigue in order to increase the security of the transactions on the Web and secure the users' account and information. Web Single Sign-On is one of the techniques that have been created to solve these issues. Unfortunately, this method creates new opportunities for hackers. The Liberty Alliance and OpenID are two of the most known Web Single Sign-On frameworks. This work intends to review the strengths and the weaknesses of both regarding their ability to protect the confidentiality, integrity and availability of the users' information, by studying their aptitude to prevent some of the most dangerous attacks on the web. The analysis of the results shows that Liberty Alliance has created a strong infrastructure in order to mitigate those attacks. Consequently, this framework protects the confidentiality, integrity and availability of the users' information more efficiently than OpenID. On the other hand, this latter shows significant weaknesses that compromises the confidentiality, integrity and availability of the users' information.

Keywords: WebSSO, OpenID, Liberty Alliance, information security, attacks.

Table of contents

1 Introduction

Web services are more and more popular. However, this success goes along with some concerns. One of them is security. Web security has a lot of different aspects and user authentication is a crucial one. On the one hand, the means used by hackers does not always require outstanding technical knowledge. On the other hand, the users get tired trying to protect their own accounts. The reasons for this are "the plethora of passwords" and "the diversity of authentication systems" that protect the users' account as described by David Talbot (2006, p.65).

One of the solutions that have been proposed to facilitate the task for the users is Web Single Sign-On (WebSSO) which allows the users "... accessing multiple sites with a single login ... " (Talbot, 2006, p. 66). The author argues that the Single Sign-On concept may lower the burden of the users permitting them to use a single password to sign on to different websites.

WebSSO is actually neither a new technique nor concept. For example, Microsoft launched its Passport system in 1999. The advantages of WebSSO are important for the users in term of usability but security is still an issue.

OpenID and the Liberty Alliance (LA) are two of the most successful WebSSO frameworks. Though their aims are similar, their implementation is different. The protocols they use in order to securely transport the authentication and authorization information between the parties is different too. These frameworks are also formed by a set of document that constitutes their foundation. This work presents a comparison between both frameworks regarding their ability to protect the confidentiality, integrity and availability of the users' information.

This comparison is based on the ability of both frameworks to prevent diverse attacks. More precisely, the strengths and the weaknesses of both to resist to these attacks will be determined. Thanks to this work, the strengths and the weaknesses of LA and OpenID to protect the confidentiality, integrity and availability of the users' information will determined.

In the first part, some important concepts for this work will be explained. In the second part both the problem and the aim of this work will be presented. Then, in the third part, the method used will be depicted. The fourth part will be dedicated to the results. Our conclusion will be exposed in the fifth part. In the seventh part, the findings of the work will be discussed. Finally some future works will be envisaged in the eighth part.

2 Background

LA and OpenID are two WebSSO frameworks. WebSSO is based on identity management models that make possible its implementation.

In the next sections, WebSSO will be defined. Then, three different identity management models and their trust requirements will be presented. The concepts confidentiality, integrity and availability of the users' information will be explained. In addition some attacks and the countermeasures against these attacks will be depicted. Finally, LA and OpenID as well as their respective Single Sign-On procedures and some of their vulnerabilities will be presented.

2.1 WebSSO

WebSSO allows the user to sign-on only once to access different web applications, improving the ergonomics and presumably the security of the Internet. Madsen, et al. (2005, p.78) indicate that "an average user today has 40 personal and professional accounts requiring usernames and passwords". While users haves to identify and authenticate themselves successively to each and every websites they visit during a working session, WebSSO spares them this tedious task.

WebSSO allows the users' authentication information to be propagated from a website (where the user signs-on) towards others. WebSSO creates a transparent and coherent system for the user, in spite of the fact that the applications are heterogeneous. It also increases the usability of the sign-on procedures. In addition, it spares the user from having to keep in mind the credentials created for each website.

The scope of a WebSSO implementation is constituted by all the websites where the users can use a Single Sign-On function. This scope depends on the identity domains created by the identity management model used.

2.2 Management identity models and trust requirements

There is a clear relationship between authentication, Single Sign-On and identity management. Madsen, et al. (2005, p. 78) define identity management as "… model of managing identities across policy and/or application domains in which the identity data is distributed but yet part of a virtual whole". The identity management model influences the trust requirements, in other words, the nature of the actors and the trust relations between them.

In this section, three different identities management models are going to be presented. The three models are the isolated identity, federated identity, and user centric identity management models. The presentation will encompass the trust requirements inherent to each model.

2.2.1 Isolated identity management model

According to O'Neil et al. (2003), it is not rare that a person has a lot of disconnected identities. Actually, one for each website they have to log-in to. In most cases, an identity is alleged by a username and authenticated using a password. In those circumstances, each website acts as an identity provider and has different requirements concerning the username and/or the nature of the password. In this case, the scope of each identity is confined to a single website. This is called "isolated identity management model" because there is no connection between someone's different identities. As a result, a user must sign-on multiple times and keep track of each username/password they own. In order to avoid that situation, some other models have been developed as we are going to explain in the next subsections.

Nevertheless, in this model, the different actors are the users and the service providers. The trust relationship that binds them is simple. The service provider determines the security policy that is applied. It fixes how the different aspects of the clients' account are secured from the technical aspects (encryption, authentication methods…) to the non-technical ones (disclosure of personal data, policy for the client...)...

2.2.2 Federated identity management model

LA uses another approach, namely the federated identity management model. Jøsang et al (2005, p. 101) defines it as "the set of agreements, standards and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within the group".

The basic idea is to link different identifiers and create a federated identity domain. In this model, "different domains/sites choose to rely on identity data/operations that are held or occur elsewhere" (Madsen & al, 2005, p. 78). Consequently, they compare the federated identity model to the passports that are issued by the government of a single country. However, the passports are valid in all the countries that have agreed on their legality.

The aim of this model is, in fact, to allow WebSSO. Each member of the group acts as an identity provider. The users must have one identity per website. In addition, they have another set of federate credentials. They use them to (single) sign-on within the domain created by the agreement between the members of the federation.

This approach adds a level of complexity due to the need and presence of a third party. This third party is an identity provider. It creates a link between the websites. When users authenticate themselves using their federate credentials, they can be automatically authenticated to all the content providers that are part of the federated domain. In this scheme, the identity provider is an asserting party because it provides the user's information to the service providers (the relying parties), using assertions.

A new trust relationship is created between the members of the federated domain. The content providers have to rely on the accuracy of the information given by the asserting party. The identity provider must trust the legitimacy of the authentication request coming from the service providers. This trust is based on the application of the agreements, on policies and procedures agreed by each of them. In addition, identities are not common in the whole federated domain. That introduces the need of mapping the identities between the members. This mapping must be initiated and consented by the user.

2.2.3 User centric identity management model

The identity management model used by OpenID, in order to implement WebSSO, is a user centric one (Smith, 2008). According to him, thanks to this model, the users have more power over their profiles. It also improves the user experience.

The users have a unique identity, valid on different websites. A common identifier domain is created. This approach allows the services of multiple third parties that are identity providers. They detain data about the users and assert their authenticity to services providers. In the case of OpenID, the third party can be either an identity provider or anyone can create an own OpenID identity using an own “URI, blog URL or website” as OpenID identifier (OpenID Foundation, 2010).

If one compares this model to the federated identity management model, these third parties introduces different trust relations. According to Smith (2008, p.9), the particularity of this model is that the trust relationship between service and identity providers is not established in advance. It is the users that both determines and indicates to the services provider which identity provider to trust. Consequently, both the users and the content providers need to trust the procedures implemented by the identity provider regarding the users registering and authentication procedures. On the other hand, the identity provider must trust the service providers and the legitimacy of their requests.

Jøsang et al (2005) explains that the main security differences between identity management models are due the difference of trust requirements. As we just saw, each model introduces some different trust requirements. As a result, each model introduces different issues concerning how the protection of the users’ information is assured.

In the next section, we are going to describe the components of the user’s information that are a concern for this work in order to explain why their protection is essential.

2.3 The component of the users’ information

Identification, authentication and authorisation are parts of identity management that aim to protect the users’ information, in a website. The three elements of information security that are a concern for this study are the confidentiality, integrity and availability (Renaud, 2007).

- Confidentiality refers to the fact that only authorised persons can access and read the information.
- Integrity refers to the fact that only authorised persons can access and modify the information. In other words, that the information is authentic and complete.
- Availability refers to the fact that the authorised persons can access the information when needed.

Breach of confidentiality, integrity and availability may have different causes; among them the behaviour of the user, disasters or different attacks against the authentication procedures of a website.

In the next section, some common attacks against the websites’ authentication procedures are going to be described. This description will be completed by a depiction of the countermeasures that should be implemented, by identity and service providers, to prevent them.

2.4 Description and prevention of some common attacks against the authentication procedures

Colomer, et al. (2006) and Madsen, et al. (2005) have identified several common and intentional identity theft attacks that aim to fool the identification and authentication procedures that protect user’s information in a website. These attacks are harmful because they can give complete access to users’ information and compromise its confidentiality, integrity and availability.

Some of them are typically technical attacks (online password guessing attacks, sniffing). Social engineering is a typically non-technical attack because it doesn't require technical knowledge in any phase of its lifetime. Finally, pharming and phishing are in the middle. Their success being based on the set-up of technical methods implemented with a psychological approach. The objective of those attacks is mainly obtaining identity information and illegitimate access to someone else's account. Therefore, when those attacks are successful they threaten the confidentiality, integrity and availability of the users' information.

In this section, we are going to define those attacks as well as the main methods of prevention against them. Then, we will describe the countermeasures that have to be implemented in order to prevent all of them.

2.4.1 Social engineering

According to Bailey (2004, p. 1), social engineering is "a technique used by hackers or other attackers to gain access to information technology systems by getting the needed information (for example, a username and a password) from a person rather than breaking into the system through electronic or algorithmic hacking methods."

Social engineering does not require the use of technical means or exceptional computer knowledge. This attack is rather based on the social competences of the hackers and on the "natural desire of humans to trust others; to assist in others labors and to gain favor in their eyes" (Bailey, 2004, p.5).

2.4.2 Prevention of social engineering

Users' education and training regarding social engineering threats appear to be the main lines of defence against this attack. Education should encompass according to Wood (2005):

- Users' awareness on this particular threat, its consequences and an overview of the methods used by social engineers.
- User guidance applied in different situations, for example what to discuss in public or how to handle passwords.

Training should concern both security awareness and resistance training in order to prepare users to resist to social pressure and other manipulative attitudes. Some technical means can nevertheless be implemented, among them multi-factor authentication and accounting. Accounting is the possibility given to the users to consult the history of their connections (Liberty Alliance project, 2005).

According to Bailey (2004), security policy addressing social engineering and tailored for each kind of audience should be created too. In addition, security audit controls must be set-up in order to control the efficiency of these measures.

2.4.3 Online password guessing attacks

Pinkas and Sander (2002, p.1) describe online password guessing attacks as attacks where the hacker, being online, tries "all possible passwords, until they find the correct one". When a password is disclosed, the hackers can access the user's account and carry out actions, as if they were the owner.

2.4.4 Prevention of online password guessing attacks

Prevention is mainly about increasing the amount of time and resources that it takes to brute force a password (Pinkas & Sander, 2002). Online password guessing attacks, according to the authors can be prevented by implementing delayed response, account locking and IP address blocking.

Delayed response slows the response of the server in order to prevent the hacker from "checking sufficiently many passwords in a reasonable time." according to Pinkas and Sander (2002, p.162). Account locking aims to block any tries that come from an IP address after a given number of unsuccessful attempts, with a particular username. Intrusion detecting systems allows the implementation of these methods of mitigation.

Others countermeasures are the encryption of both the password and the identifier and multifactor authentication (Landau, 2003). A password policy destined to the different kind of users is necessary as well. The SANS institute (2006) has edited a password policy that will be used as a basis for this work. This policy describes among others the current passwords protection standards. Finally, once again, security audit controls must be set-up in order to control the efficiency of these measures.

2.4.5 Sniffing

Sniffing is the "use of a network interface to receive data not intended for the machine in which the interface using a packet-sniffer" de Vivo, et al. (1997). The aim of sniffing is often to illegally get access to information about credentials.

2.4.6 Prevention of sniffing

Prevention of sniffing concerns, first and foremost, encryption as it renders the sniffed data useless. King (2006) describes it as "the most viable form of packet-sniffing protection".

Furthermore, the implementation of different techniques of authentication like, one time passwords or strong identification diminishes the success rate of this attack.

2.4.7 Phishing and pharming

Phishing and Pharming are very similar in their conception as well as in their aim. According to Srivastava (2007), both use social engineering and technical resources to persuade users to divulgate sensible information via counterfeit websites. These latter imitate a legitimate website where the user uses to log-in.

Phishing is achieved by first sending emails to multiple users persuading them to click on a link. The latter gives access to a counterfeit website. The phisher can also use the e-mail to install malicious programs on the user's computer.

Pharmers do not employ e-mails in order to contact and deceive their victims. Instead, they employ techniques like hosts file modification, DNS cache poisoning, domain hijacking, static domain name spoofing or malware to redirect the traffic to their counterfeit websites. The pharmers use malicious codes, like viruses or Trojan horses, in order to compromise the host and allows the success of those techniques.

The consequences of these two attacks are nevertheless the same: the user is misled into divulging sensible information like passwords.

2.4.8 Prevention of phishing and Pharming

Srivastava (2007, p. 22) indicates that "Employee/customer education and awareness" are the most important factors to prevent these attacks. This is achieved by implementing policies that provide indication on how to detect and react to these attacks. Furthermore, according to the CPNI (2010), the methods used by the pharmers and the phishers, as well as their consequences must be taught.

Technology completes the defences. According to the CPNI (2010), that includes:

- Blocking malicious web traffic, filtering spam emails.
- Detecting and removing malicious software.
- Blocking sensitive information from leaving the corporate network.
- Patching network infrastructure.
- Hardening network infrastructure.
- Using SSL/TLS.
- Cryptographic signing of digital communication and certificate.

2.4.9 The countermeasures that must be implemented to prevent the attacks.

The previous subsections allowed us to determine the countermeasures against each attack. These countermeasures are summarized in this subsection. In addition, the particular criteria that will be considered for the comparison of LA and OpenID are exposed in the following lines. The strengths and weaknesses of both, to resist to attacks, will be estimated by comparing the countermeasures that are required by both frameworks, to the criteria listed in the following lines.

According to the CPNI (2010), the policies should be updated frequently and supervised by both policy and security specialists. Furthermore they should be written and communicated by communications expert. Finally, they must be clear and adapted to each audience.

In order to compare the policies of both frameworks, we will examine the following points:

- How the organization is concerned by security and what actions are taken to guarantee it, at the organizational level?
- Does the organization have and advocate clear security policies adapted to each type of audiences regarding the diverse type of threats. In order to determine the quality of the policies, some factors like the guidelines used or the author of the policies will be taken into account.
- How often the policies are updated?

The detailed study of the policies, if any, would allow us to determinate if they are written to be able to fight the following threats: online password guessing (password policy), social engineering in general (that would include pharming, phishing and the others attacks.). In other words if they:

- Comply with the document edited by the SANS institute (2006).
- Indicate how often to upgrade firewalls, anti-virus software and others security programs.

- Describe what to do if a security problem is discovered or suspected.
- Describe how the company will communicate and what answer should never be provided.
- Recommend security audit scheduled on periodically basis or randomly, like the one described in Bailey's article (2004).

Technical countermeasures refer to the study of the features and devices that the members must implemented to prevent the attacks. Here are the different points that will be checked:

- How secure are the channels between the user, the identity providers and the service providers regarding the exchange of credentials.
- Which data are encrypted (password, identifier, all data between the different actors) and with which level of encryption.
- What are the possibilities to use one time passwords or other strong authentication methods.
- What are the obligations of the identity and service providers regarding the implementation of intrusion detection systems and firewalls.
- What means are used by the identity and service providers to authenticate themselves.

In this section, several attacks against the websites authentication's procedures have been studied. We have determined the main countermeasures that should be implemented by the members of the frameworks to prevent them and consequently to guarantee the security of users' information. In the next section, some specific terminology will be explained. Then, LA and the OpenID frameworks will be presented as well as their respective Single Sign-On procedures and some of their vulnerabilities.

2.5 Presentation of LA and OpenID

In this section, some specific terms will be explained. After that, LA and OpenID as well as their Single Sign-On procedures will be presented. In the meantime, some security issues of both will be described.

2.5.1 Terminology

A Circle of trust: A circle of trust (figure 1) defines the contractual bounds between service providers and identity providers within an LA federation. This circle is based on agreements that defines the information that the different entities will share and how, according to Sheckler and Varney (2005).

A principal: A principal is an entity that can acquire a federated identity. It may be a person, a group of persons or a company. The principal interacts with the identity and service providers via a user agent or a client, most of the time a web browser (Sheckler & Varney, 2005).

An Identity provider: An Identity provider is an entity that creates, maintains, and manages identity information for users. It also provides users' authentication to other service providers according to Sheckler and Varney (2005).

A Service Provider: A Service Provider is an entity that provides online services to a user. It is usually a website (Sheckler & Varney, 2005).

SAML: SAML refers to SAML 2.

A SAML assertion: An SAML assertion can be described as authentication, attribute and entitlement information produced by a SAML authority about a principal (OASIS, 2005).

OpenID: The term OpenID defines either the Web Browser SSO protocol, the users' OpenID identifier or the whole framework that includes all the specifications (Recordon, 2007).

An OpenID provider: An OpenID provider is an identity provider dedicated to OpenID (OpenID explained, n.d.).

A relying party: A relying party (RP) is an OpenID enable service providers (OpenID explained, n.d.).

2.5.2 The LA Framework

LA framework, also known as the Liberty Alliance Project, was created in 2001. It assembles actors of the industrial, IT, banking and governmental world under the shape of a consortium. The objective is to define a set of specifications and protocols for federated identities and communication between web services. These protocols can be implemented within the framework of deployments intra-domain as well as inter-domains.

The ambition of LA is to "conduct online transactions while protecting the privacy and security of identity information" according to the Liberty Alliance Project (2010 b). LA claims that there are "…more than one billion liberty-enable devices and identities…" (Liberty Alliance Project, 2010 b).

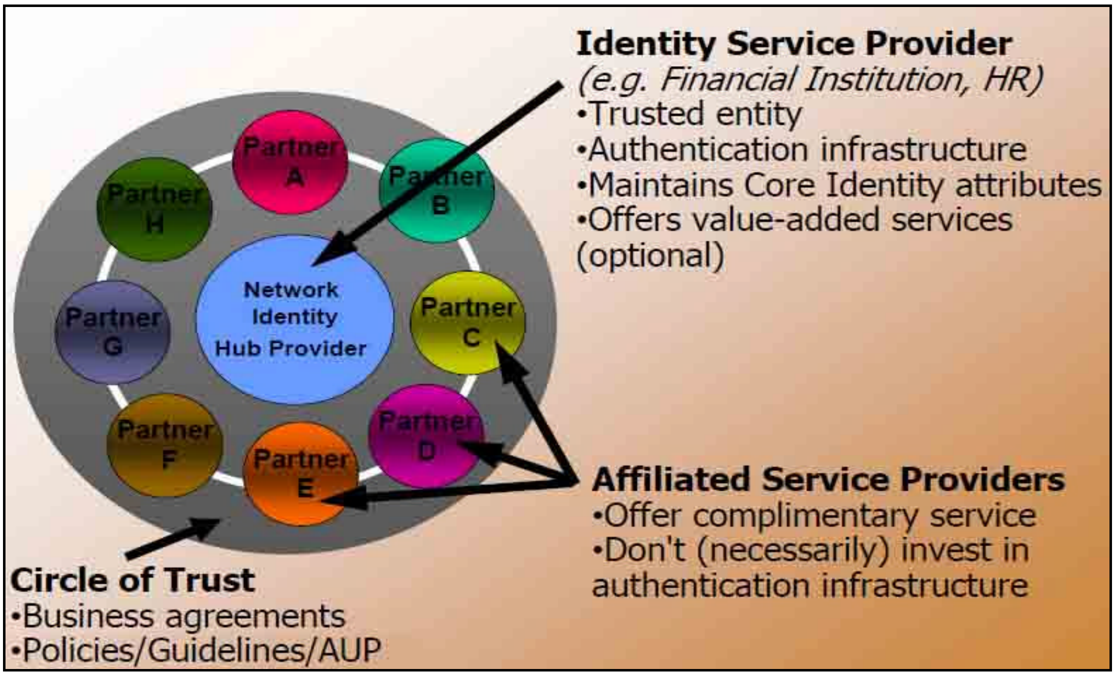
Identity Service Provider
(e.g. Financial Institution, HR)
•Trusted entity
•Authentication infrastructure
•Maintains Core Identity attributes
•Offers value-added services (optional)
Partner A
Partner B
Partner C
Partner D
Partner E
Partner F
Partner G
Partner H
Network Identity Hub Provider
Affiliated Service Providers
•Offer complimentary service
•Don't (necessarily) invest in authentication infrastructure
Circle of Trust
•Business agreements
•Policies/Guidelines/AUP

Figure 1 : The "Circle of trust" model (Liberty Alliance Project, n. d.)

2.5.3 Single Sign-On procedure of the LA

Users who want to Sign-in to service providers (who are members of an LA's circle of trust) have several steps to accomplish.

At first, the users must choose one or several identity providers as well as register themselves to different service providers (who are member of the same circle of trust).

Then, the users must explicitly federate their accounts, in other words link their identity provider accounts with their account at a given service provider. The principal must achieve this procedure for each service provider where single sign-on is to be enabled. When all these phases are completed, the principal possesses two accounts at the service providers, a normal one and a federate one (Figure 2). At that point, the principal is able to sign-in to the identity provider.

Finally, the users choose a service provider. This one sends back an authentication request to the user agent that redirects it to the users' identity provider. If the users were previously authenticated (figure 3), the identity provider redirects them to the service provider and send to the latter an authentication assertion. If the users were not authenticated, they are invited to do so and the identity provider acts as previously explained. Finally, the service provider receives the authentication assertion, checks its validity and allows the service. For the record, principal keeps the possibility to log-in to a given service provider using their service providers' account.

2.5.4 The main Security issues of LA Single Sign-On procedure

Technically, authentication information between principals, identity providers and service providers is exchanged using assertion (contained in security tokens) provided by the Security Assertion Mark-up Language (SAML). SAML is a protocol based on XML. SAML is used to communicate users' information between identity and service providers. It allows the interactions between domains that use different authentication methods (D'Costa-Alphonso & Lane, 2010; Lewis & Lewis, 2009). The service providers send authentication requests to the identity provider that respond by sending authentication assertion (OASIS, 2005). According to Jøsang et al. (2005), identity and service providers trust each others assertion.

Jøsang et al. (2005), underlines that sufficient authentication mechanisms must be implemented by the identity provider. That is, the sign-on procedure at the identity provider must be protected against all the attacks that are studied in this work. On the other hand, the diverse members must prove their identity using effective methods as we are going to explain.

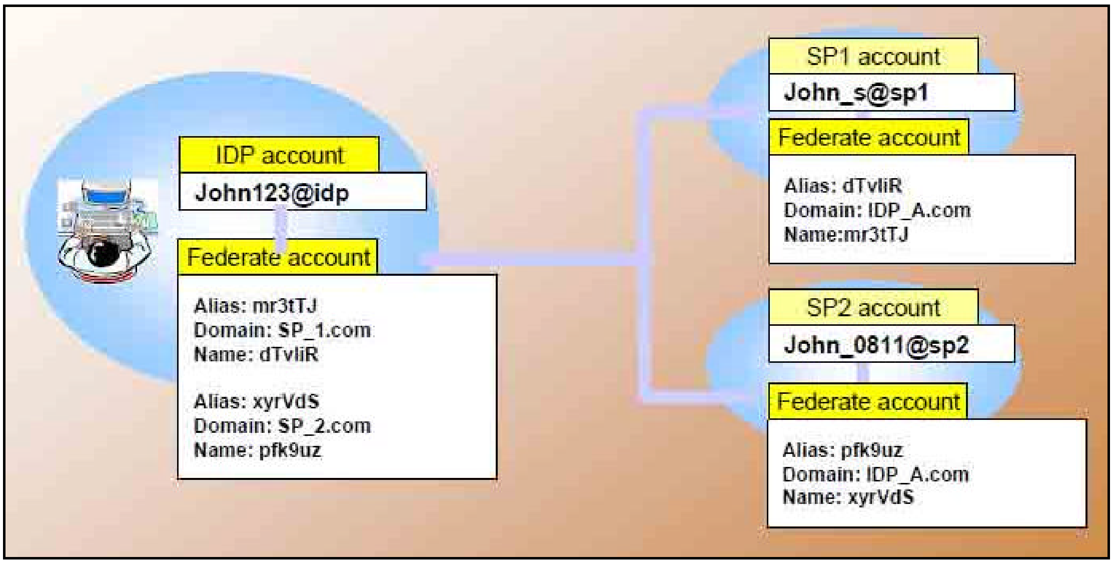

Figure 2 : Account Linking and Identity Federation (Liberty Alliance Project, n. d.)

The use of digital signatures and certificates, for example, render a rogue service provider unable to authenticate itself to an identity provider. Furthermore, the communication channels used to send the assertions must be protected from sniffing as they may contain authentication information.

Finally, the users must handle their credentials carefully. They highlight that the identity provider must, consequently, provide the principal with recommended practices and policies.

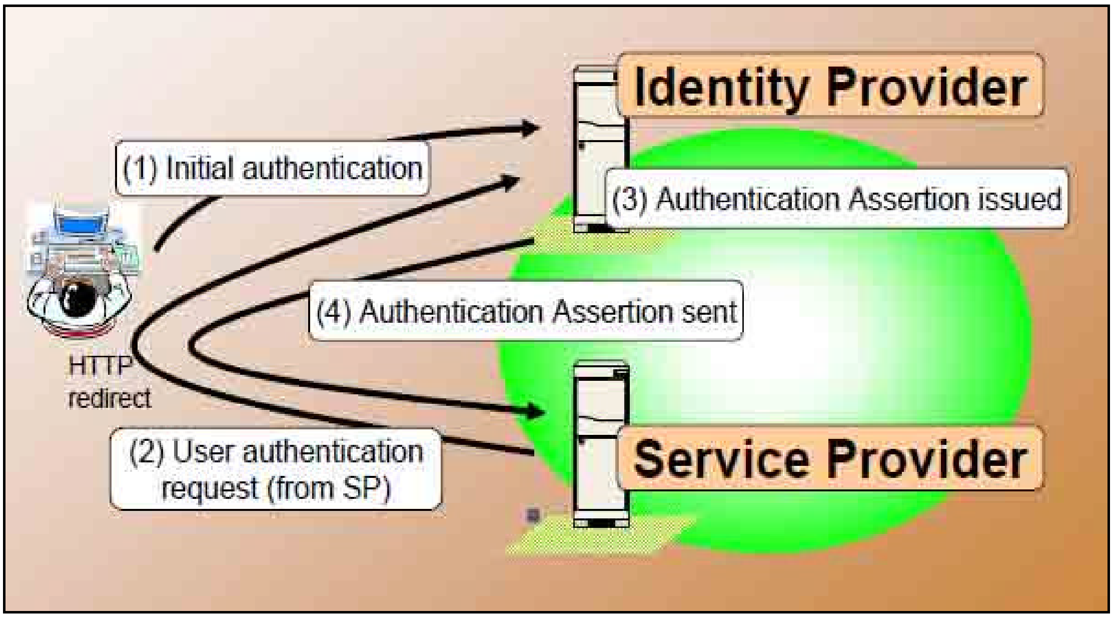
Identity Provider
(1) Initial authentication
(3) Authentication Assertion issued
(4) Authentication Assertion sent
HTTP redirect
(2) User authentication request (from SP)
Service Provider

Figure 3 : Single Sign-on from a service provider (Liberty Alliance Project, n. d.)

2.5.5 The OpenID framework

Created in 2005, this project aims to allow users using "…an existing account to sign-in to multiple websites, without needing to create new passwords" (OpenID Foundation, 2010). It permits also WebSSO. It is based on the use of decentralised identity providers that detain the users' sign-on information in place of the diverse content providers. The users just authenticate themselves to their identity provider that confirms their identity to the visited websites.

According to the foundation, there are "over one billion OpenID enabled user accounts and over 50 000 websites accepting OpenID for logins". Furthermore, some important organisations like Microsoft and France Télécom issue and/or accept OpenID identities. OpenID is both an authentication protocol and its implementation.

2.5.6 Single Sign-On procedure using OpenID

Users must obtain an OpenID from an OpenID provider. OpenID has a decentralized system. Thus, the users can register themselves to any OpenID provider. The identity provider supplies the user with an OpenID which is actually a URL (OpenID explained, n.d.). Once done, the users can sign-in using their OpenID account to OpenID enable service providers. On the contrary to the LA's protocol, the user just has a set of credentials that can be used on different OpenID enabled service providers.

To single sign-on, the users identify themselves to a service provider, with their OpenID. The service provider asks the identity provider to authenticate the client (redirection). If the client is already authenticated, the identity provider grants access.

Otherwise, the users are prompted to authenticate themselves (Tsyrklevich & Tsyrklevich, 2007). The figure 4 explains the technical implications of the process.

2.5.7 The main Security issues of the OpenID Single Sign-On procedure

According to Tsyrklevich and Tsyrklevich (2007), this protocol presents some security issues. During the first step (figure 4), the service provider and the identity provider can be victims of phishing and/or pharming. The second step consists in downloading OpenID URLs. The authors describe this step as very risky. The service provider must control carefully this phase in order to be prevented from downloading malicious contents. The third steps correspond to the exchange of crypto keys in order to guarantee the integrity of the data between the identity and the services providers. Man-in-the middle attacks can occur here.

The fourth step result in the user's redirection to the identity provider. Attacks like phishing and pharming can take place here. The authors stipulate that malicious service providers can redirect the users to fake identity providers in order to steal the users' credentials. Tsyrklevich and Tsyrklevich (2007, p. 9) clarify that "phishing is a well known attack against OpenID protocol and remains unsolved".

During the fifth and the sixth steps, the users authenticate themselves using their credentials. Attack like online password guessing, and sniffing can take place here. Finally, throughout the last step, the user is redirected back to the service provider. The most probable attack here is sniffing that would permit replay attacks.

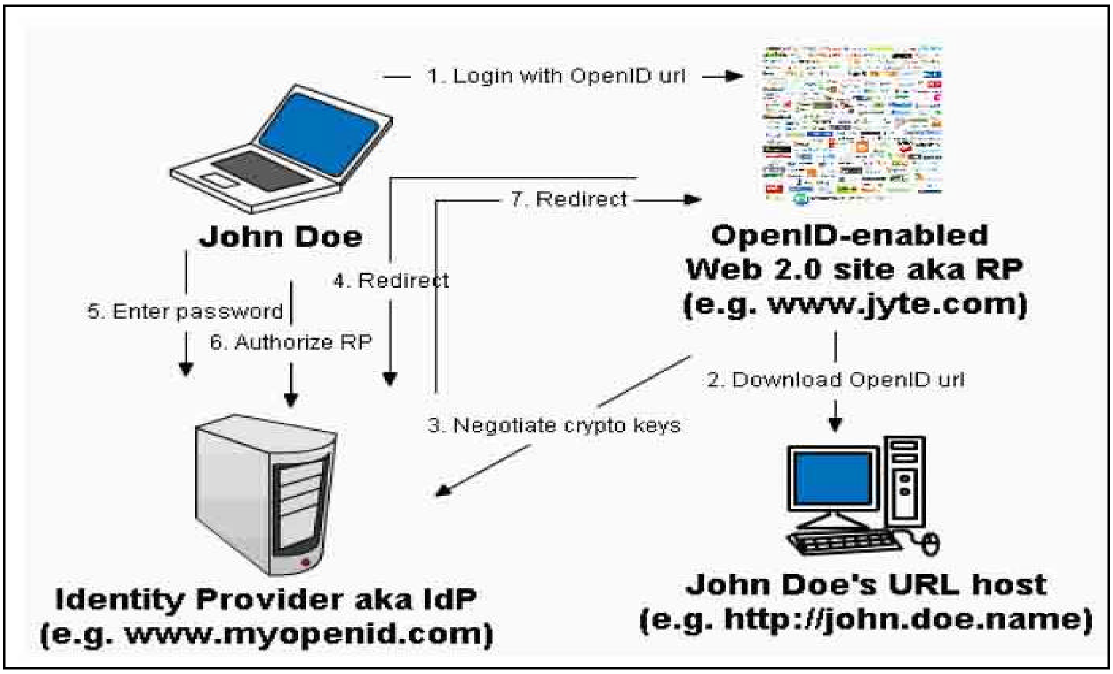
1. Login with OpenID url
John Doe
7. Redirect
OpenID-enabled Web 2.0 site aka RP (e.g. www.jyte.com)
4. Redirect
5. Enter password
6. Authorize RP
2. Download OpenID url
3. Negotiate crypto keys
Identity Provider aka IdP (e.g. www.myopenid.com)
John Doe's URL host (e.g. http://john.doe.name)

Figure 4: The OpenID protocol (Tsyrklevich & Tsyrklevich, 2007)

3 Problem and aim

When a WebSSO solution is to be implemented, the choice is often made between an LA implementation and OpenID. LA and OpenID frameworks present some similarities as they both allow, among other things, WebSSO. However, their approaches are not identical: they are based on different identity management models, trust requirements and technologies.

The first objective of WebSSO is the simplification of the authentication procedures for the users. These procedures mainly aim to protect the users' information. The way they are implemented influences the security of the users' information. Regarding LA and OpenID, those procedures depend on the technologies implemented, the identity management system used as well as a set a documents. Those diverse components constitute the foundation of both frameworks (Jøsang et al 2005; Smith, 2008).

The technologies aim to allow WebSSO. They mainly aspire to secure the exchange of the users' authentication and authorization data between partners. The identity management system determines the nature of the partners and the relationships between them. The documents are among others specifications, guidelines, best practices, policies and/or policy guidelines. They regulate the conditions under which the protocols must be implemented.

Liberty Alliance is based on a federated identity model and relies mainly on the Security Assertion Mark-up Language (SAML) in order to secure the exchange of users' authentication and authorization data between partners. In 2005, SAML technology was operational and its standards were approved (Smith, 2008).

In the same year, OpenID was created which is based on a user centric identity management model. Furthermore, OpenID relies on its own technology, the OpenID protocol, to secure the exchange of users' authentication and authorization data. OpenID's popularity has grown ever since and has become the principal challenger of LA.

Smith (2008) has studied the trust relationships inherent to both frameworks. Smith (2008, p.9) asserts that the key advantage of OpenID compared to LA is that "the trust relationship doesn't have to be set up in advance". The trust relationship in LA is established in advance by the agreements that bind the diverse partners. The author concludes on the advantages of both frameworks, for the user, in terms of usability. However, this article does not study the consequences of the differences between both frameworks regarding the security of the users' information.

SAML and the OpenID technology have been compared before. Hodges (2009), in his whitepaper, proposes a detailed comparison of both protocols. The results of this work regard the technical aspects, the information security as well as their ability to protect the users' information.

However, as explained previously LA and OpenID are more than technology, they are frameworks. As such, the study of some of their other components is important to determine their efficiency to protect the users' information. Indeed, the specifications, guidelines, policies, policy guidelines and the identity management system have an influence on the security of the users' information. As a matter of fact, there is a relationship between information security and identity management. This relation is "focused on three distinct areas: authentication, access management, and compliance…" (Suess & Morooney, 2009, p. 36). The authentication part is, as they describe, “central to security” and based to a certain extent “on the policies and procedures of the management system”. The problem is that the later points are not taken into account by the comparison between the SAML and the OpenID protocols.

LA and OpenID propose different way of implementing WebSSO. The security of user information must be guaranteed when WebSSO is implemented. The difference of approaches of both frameworks induces some differences in term of performance, usability and security. These latter points as well as their position on the market are the main factors that justify the choice of OpenID and LA regarding this work. Furthermore, it appears that an analysis of the whole frameworks is relevant in order to evaluate their aptitude to protect the users’ information.

In this work, we will compare Liberty Alliance and OpenID in order to establish their strengths and weaknesses regarding their abilities to ensure the availability, integrity and confidentiality of the user’s information they intend to protect.

Evaluating how both behave in security matters compared to the conventional method (one username, one password and sign-on for each visited website) is an important issue that has been covered many times. However, discussing their strengths and weaknesses compared to each other is significant because it gives up-to-date information and a foundation for decision-making related to the implementation of the one or the other method.

Intentional attacks constitute important threats against the users’ information according to Colomer, et al. (2006) and Madsen, et al. (2005). They have identified several common attacks that aim to fool the authentication mechanisms that protect the users’ information. These attacks are pharming, phishing, social engineering, online password guessing, and sniffing. Thus, our comparison is based on the analysis of the resistance of both frameworks to these common attacks.

In a first step, the security issues of both frameworks regarding the attacks have been analysed.

Then, the most prevalent countermeasures against the attacks have been reviewed. The level of compliance to these countermeasures has been used to determine the strengths and weaknesses of both frameworks regarding the attacks.

In addition, both the SAML and OpenID protocol have been compared in order to describe the means that they use to protect the confidentiality, integrity and availability of the users’ information from the attacks. This point is important because the security of the technology employed constitute an important component of those systems.

Along with the guidelines, the specifications, diverse papers on the topic and best practices, the policy guidelines concerning the security in LA and OpenID have been studied, as they are essential. For example, Wood (2005) claims that policies are the first countermeasures that should be implemented against social engineering.

Those steps allowed us to determine at first how both LA and OpenID prevent the attacks. Then, we were able to establish the strengths and the weaknesses of the frameworks to resist to the attacks in question. In the end, we were be able to deduce and then compare the strengths and weaknesses of LA and OpenID to protect the confidentiality, integrity and availability of the users’ information from their strengths and weaknesses to resist to the named attacks.

4 Method

Different methods can be used in order to compare the strength and the weaknesses of both frameworks. A case study seems to be a conceivable choice because it could give detailed information about realised attacks, if any. However, it would not enlighten much about all the risks. On the other hand, according to Berndtsson, et al. (2008) the study would be limited both in time and scope (concerning LA as we would have to limit ourselves to one of its implementations). A literature analysis seems to be more accurate. It will give information about both realised attacks during a long period of time, failures and vulnerabilities.

Accordingly, the resistibility of LA and OpenID to common attacks has been analysed. More precisely how both systems resist to phishing, social engineering, online password guessing, pharming and sniffing attacks. The study has encompassed an analysis of the technical solutions inherent to both models, as well as the investigation of the policies, guidelines, specifications, best practices and several papers on the topic.

The first step has been the analysis of the security issues of both frameworks regarding the attacks. This study was mainly based on three documents: Jøsang et al. (2005), Tsyrklevich and Tsyrklevich (2007), and finally the Liberty Alliance Project (n. d.).

Then, the most prevalent countermeasures against the attacks have been listed to be able to define the strengths and weaknesses of the frameworks to resist the attacks. This study has been based on documents written by Bailey et al. (2004), Pinkas and Sander (2002) as well as documents issued by the Centre for the Protection of National Infrastructure (2010) and the SANS institute (Srivastava, 2007).

In addition, the comparison between SAML and the OpenID protocol has been made principally thanks to Hodges whitepaper's (2009). The Lewis and Lewis' article has been used in order to complete the picture regarding LA. Concerning OpenID, the OpenID's website (OpenID Foundation, 2010) gave us access to diverse specifications of this framework. The analysis has been focused on the countermeasures that must be implemented by the members to prevent the different attacks.

The next step has been accomplished by the analysis of the policy guidelines, guidelines, specifications and others documents published on LA and OpenID's websites as well as diverse papers that examine them.

Those steps allowed us to review how both LA and OpenID prevent the attacks in question.

Then, we deduced the weaknesses and the strengths of LA and OpenID to resist to the different attacks. The different attacks have this particularity that they endanger, at different levels, the confidentiality, integrity and availability of the users' information. Therefore, we were able to map and finally compare the strengths and the weaknesses of both frameworks to resist to the attacks to their ability to protect the confidentiality, integrity and availability of the users' information. The results are presented in the next part.

5 Results

In this chapter, we will present how LA then OpenID prevents the attacks. We will use the explanations presented in the section 2.4.9. For each framework, we will describe first the overall philosophy regarding security. Then, we will expose the intra protocol security (the security features inherent to each single sign-on protocol). Next, we will present the extra protocol security (the security features of each identity provider or service provider's own infrastructures). In addition, we will analyse the strengths and the weaknesses of both frameworks to resist to the attacks. Thanks to this analysis, we will finally describe and compare their ability to protect the confidentiality, availability and integrity of the users' information.

5.1 Prevention of the attacks by LA

Security has been a major concern for LA since the beginning of the project. The Liberty Alliance Project releases, on regular basis, guidelines and best practices to allow the members to update their security policies as well as the security of their infrastructures. Meanwhile, some groups and organizations have been created by LA in order to improve the security. LA has also edited several documents to help the identity and service providers reach an appropriate level of security. Those documents and workgroups illustrate the overall philosophy of LA regarding the security of the framework.

In this section, the LA's most prevalent security groups and documents will be presented. Then a detailed description of the countermeasures required by the framework will be exposed first regarding the security intra protocol then regarding the security extra protocol.

5.1.1 The LA's most important security groups and documents

The Public Policy Exp Group: The Public Policy Exp Group (PPEG) is composed by policy experts from around the world. This organisation works to provide up-to-date guidelines and best practices for privacy, to all LA's members (Liberty Alliance Project, 2010 a). Their recommendations are included in the LA policy guidelines that aim to protect end users' identities and enforce security.

The Identity Theft Prevention Workgroup: The "Identity Theft Prevention Workgroup" has been formed by LA to specifically address the problems of identity theft and online fraud. This group has edited a Whitepaper in 2005, The Identity Theft Primer, "to collectively address the technology and policy issues surrounding online fraud and identity theft" (Liberty Alliance Project, 2005).

The Deployment Guidelines for Policy Decision Makers: The Deployment Guidelines for Policy Decision Makers (Sheckler & Varney, 2005) is the main paperwork that rules the deployment of Circles of Trust. It defines the basis of the trust relationships between members thanks to guidelines and best practices.

The Liberty Identity Assurance Framework: The Liberty Identity Assurance Framework (Cutler, 2008) describes the security requirements that are not related to the LA protocol deployment. That concerns features such as the implementation of firewalls. It also describes how LA manages to verify if the members comply with security standards.

The Liberty Security Framework: The "Liberty Security Framework" (Champagne & Thompson, 2004, p. 16) describes how channels and messages between identity providers, service providers and user agents are secured.

The countermeasures that we are going to present are described in those documents. At first, we will describe how LA intends to neutralize the different attacks regarding its protocol. Then, the solutions that the different members of a circle of trust have to implement, in order to secure their own infrastructures and the method employed by LA to guarantee that these solutions are operational, we'll be exposed.

5.1.2 Intra protocol security

In this subsection, we will study which of the diverse countermeasures (presented in the subsection 2.4.9) are to be implemented by the members of a circle of trust. Issues regarding the communication channels, the data encryption, the authentication of the identity and service providers, the security features of SAML, the qualities of the credentials and some prevention features against social engineering will be studied.

Communication channels and encryption: According to Champagne and Thompson (2004), channels security refers to how the communication between the different actors is protected. The figure 3 (p. 11) shows the main communication channels in question. They principally concern the communication between the principal, the identity and the service providers but also some intermediary proxies.

These different partners must send messages to each others to enable Single Sign-On. Message refers to either the SAML assertions that carry Single Sign-On authentication information or the service providers' requests. Table 1 summarizes the requirement of LA. At least TLS1.0 or SSL3.0 must be used for security channels. All messages must be exchanged through these security channels. Uberti (2005) underlines that all the communications between the users, identity providers and service providers (more generally between recipients and senders) must be integrity and confidentially protected using SSL 3.0 or TLS 1.0.

Table 1: Liberty security mechanisms (Champagne & Thompson, 2004)

Security Mechanism	Channel Security	Message Security (for Request, Assertions)
Confidentiality	Required	Optional
Per-message data integrity	Required	Required
Transaction integrity	-	Required
Peer-entity authentication	Identity provider – Required Service provider - optional	-
Data origin authentication	-	Required
Non-repudiation	-	Required

Besides, LA standard stipulates that it should not be possible to repudiate the different messages (Duserick & Fidelity Investments, 2004). In other words, in case of fraud, the identity and the service provider where the theft signed-on can be identified. Thus, members are more entitled to both cooperate and to scrupulously follow the different policies and recommendations regarding security to disengage their liability in case of fraud. Furthermore, actions to help a failing identity or service provider can be taken more accurately. This is called "coordinated response to incidents of frauds" (Duserick & Fidelity Investments, 2004, p.9).

The authentication of the different actors: Mutual Authentication must be implemented. The messages between identity providers and service providers must be "...digitally signed and verified..." in order to ensure "...data integrity, data origin authentication, and a basis for non-repudiation" (Champagne & Thompson, 2004, p. 11). Thus, the signing and verification of protocol messages must be done with certificates and private keys that are different from the ones used for the communication channels.

Moreover, each identity provider must be preconfigured with the list of the service providers that belongs to the same circle of trust and vice versa before engaging interaction. In addition, the identity providers must authenticate themselves (with a certificate for example) before requiring any authentication from the users. Finally, received responses must correspond to send request. A mechanism that the organism may choose, in order to avoid replay, must be implemented.

Regarding phishing and pharming, Madsen et al. (2005, p. 81) state that "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". The methods used in order to create this "provider-provider" authentication determines, partly, the success or not of attacks like phishing.

SAML: According to Hodges (2009) "SAML was designed with security and modularity as its design centers". It is a protocol created to transport authentication and authorization information under the form of assertion. It supports different protocols and authentication methods as well as varied use-cases. Besides, it can be tailored to support the specific needs of the companies regarding security. The security measures are presented in a detailed specification (Hirsch, Philpott & Maler, 2005). It is required from the different members to respect the diverse standards and best practices, in order to mitigate all the known attacks (Hodges, 2009).

The quality of the credentials: The use of opaque identifiers is mandatory. An opaque identifier is not related to the user's real identity and is neither issued by an administration. This diminishes the possibility to correlate the identifier to a person (Duserick & Fidelity Investments, 2004). In addition, it is sent through secured communication channels in order to help to fight back online password guessing attacks.

Strong authentication can be implemented. Service providers have the opportunity to require other means of authentication than password. They can require authentication technologies like smartcard or pre-paid mobile login, biometric, etc. Strong authentication can be a unilateral decision of a service provider. However, it can also "be established as part of the contractual arrangements of the circle of trust" (Champagne & Thompson, 2004, p. 13). Each service provider can indicate, to the identity providers, which method they require. On the other hand the identity providers must indicate, in details, which one have been used for a session.

Prevention against social engineering: The users can limit the scope of the transactions and authorize which information is available using the Single Sign-On function. In other words, they can determine which operation only can be done at a given service provider when they are directly logged-in, using the service provider credentials (Duserick & Fidelity Investments, 2004). This measure intends to protect the users that may divulge their Single Sign-On credential to family members or unwillingly.

A weakness of single sign-on can be summarized by the expression “key to the castle” (De Clercq, 2002, p.43). That is, a set of credentials give potentially access to all information from multiple websites. According to Duserick and Fidelity Investments (2004), the former measure “reduces the scope of activity that can be conducted via identity misuse”. This is also a safeguard against other techniques that would allow attackers to obtain the Single Sign-On credentials illegitimately.

The last point concerns the accountability. LA’s identity and service providers must provide details to the principals regarding their connections. Champagne and Thompson (2004, p.4) call that function “authentication status”. They underline that the principals should be able to check their current authentication status as well as the history of their precedent sessions.

5.1.3 Extra protocol security

Champagne and Thompson (2004, p. 11) stipulate that “Many of the security mechanisms mentioned above, for example, SSL and TLS, have dependencies upon, or interact with, other network services and/or facilities such as the DNS, time services, firewalls, etc”.

The way these network services and/or facilities are implemented influences the security of an entire federation. The implementation of firewall, intrusion detection system among others is required to mitigate pharming for example.

LA proposes guidelines and best practices regarding the security of the identity and the service providers’ own infrastructures. However, the different members of a given Circle of Trust must agree on these issues. Sheckler and Varney (2005) underlines that “What are each of the Members’ security practices, including system security, trustedness/validity of the data collected, personnel policies, and organizational practice” are intern to the Circle of Trust. Nevertheless LA intends to guarantee that the different members of a circle of trust meet some requirements.

Certification of the Identity and the service providers: The Identity Assurance Expert Group (IAEG) has been formed in order to “…create a framework of baseline policies, business rules, and commercial terms against which identity trust services can be assessed and evaluated” according to Cutler (2008, p. 5). As a result, accredited auditors must certify the identity and the service providers of each Circle of Trust, as well as, the federation they form.

The four levels of certification: Cutler (Cutler, 2008) also describes the qualification of the auditors or assessors, as well as, the criteria on which the certifications are based. They are actually four different levels of certification. They are based on the four levels of insurance provided by the U.S. National Institute of Standards and Technology (Burr, Dodson & Polk, 2006). The different levels from level 1 to 4 are exposed table 2.

This approach aims to create standards to determine the trustworthiness of the different members of a circle of trust. The assurance levels are based on different criteria. One of them is the Information Security Management (ISM) that refers to the IT security of the company.

Table 2: Four Assurance Levels (Cutler, 2008)

Level	Description
1	Little or no confidence in the asserted identity's validity
2	Some confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

The level 1 requires that members:

- Account for the legality, trustworthiness, liability of their business.
- Account for online password guessing, introduction of malicious code, out-of-band attacks, spoofing of system elements/applications,
- Account for the way how the company applies appropriate controls.
- Account for the resistance strength of passwords, against online password guessing attacks.

From the level 2, the technical security must include a number of features and effective security policies. That is:

- The company must document all security measures related administrative, management, technical procedures and policies. All of them must respect recognised "…standards or published references…" (Cutler, 2008, p. 17 In addition, the policies must be "properly maintained".
- The member must put into operation an effective risk management procedure.
- Internal and independent security audit must be performed on regular basis (at least every two years). Accredited auditors should perform the independent audits with regard to both the technical countermeasures along with the quality of the policies.
- Technical means, as well as, security policies must be implemented in order to prevent Eavesdropper, replay, and online password guessing attacks.
- Both the identity and the service providers must prove their identity, legitimacy, address, financial resources among others. As a result, the company must certify that it is a "legal and operational business entity within its respective jurisdiction or country" (Cutler, 2008, p. 13).
- The companies must log each relevant security event (regarding WebSSO or not) with timestamp. The company must keep the log files, at least, for the legal period (depending of the legislation of the country).
- Moreover, the communication between different sites of a member must be secured. All remote communication "over a public or unsecured network with other service components…must be cryptographically authenticated" (Cutler R. 2008, p 21). This must be achieved using at least, the level 2 of the Federal Information Processing Standard as described by Burr, Dodson and Polk (2006).
- The organisation must have a specified keys and credentials management.
- Finally, at level 2, the members must have a specific credential policy. The term credential here encompasses both users credential as well as SAML

assertions. The credential policy must describe, at least, how the company implements the countermeasures against password guessing, message replay, eavesdropping, introduction of malicious code, spoofing of system elements/ application, out-of band attacks (social engineering) and ”apply control them to acceptable risk levels”(Cutler, 2008, p.60).

- Regarding the policies, the companies are recommended to apply the advice and recommendations of the Deployment Guidelines for Policy Decision Makers (Sheckler & Varney, 2005, p. 9). The section 4 of this guideline concerns the security. It is indicated that the members “...should take reasonable steps to protect and provide an adequate level of security…” regarding online fraud.
- The different points that the policies must consider concern “management/time out requirements, levels of encryption, strength of authentication mechanisms used, invalid password attempts lockout, lockout intervals, conditions such as hours of allowed access or source IP addresses/firewall rules, practices around authorized personnel, auditing frequency and areas, forced password change frequency, password minimum standards, practices for validating user before password resets, procedures for validating data, especially that used for entitlement, and software change management practices.” (Sheckler & Varney, 2005, p. 9).

  The members are recommended to follow some international security standard, like ISO 17799, as a baseline. The authors stress the necessity to update the policies and the technologies in order to be able to fight new threats or risks.

At level 3 and 4, the requirements are more specifics and the policies and practices regarding the security are described more in details. In addition, they are more stringent. Among others, at level 4 the IT management methodology must be in “compliance with code of practice ISO/IEC 17799.

The second level of this framework does not specify, in detail, what the members must implement neither how but just the result to reach. Nevertheless, from this level, all the countermeasures against the attacks in question must be implemented efficiently. The third and fourth levels offer a better prevention. The certifications and regular and independent audits aim to guarantee the members’ compliance to a given level of security. Federations that have no IAEG certification are not LA federations.

In the next section, we will present how OpenID prevent the attacks studied in this work.

5.2 Prevention of the attacks by OpenID

The OpenID framework is defined by six technical specifications. None of them is specifically dedicated to the security. Only some of them contain chapters regarding this specific topic. Hodges (2009) describes the OpenID framework as easy to deploy. According to him, this is due the philosophy that grounds the project: “trust and accept all comers.” This philosophy has, as we are going to explain, important consequences on the security of OpenID.

In this section, the countermeasures required by the OpenID framework will be exposed first regarding the intra protocol security then regarding the extra protocol security.

5.2.1 Intra protocol security

In this subsection, we are going to study which of the diverse countermeasures presented in the subsection 2.4.9 are required by the OpenID framework. Issues regarding the communication channels, the data encryption, the authentication of the identity and service providers, the qualities of the credentials and the prevention features against social engineering will be studied

Communication channels and encryption: The use of secure channels is not mandatory. The OpenID Authentication 2.0 (Recordon, 2007) expresses concerns about the use of secure features like digital signatures and digital certificates. He advises that "SSL with certificates signed by a trusted authority" should be employed. This is important especially for the interactions between the identity and the service providers but also with the user agent. On the other hand, Recordon and Fitzpatrick (2006) explain that HTTP can be used during the authentication phase even if HTTPS is recommended.

To guarantee the integrity of the data exchanged between the identity and the service providers, OpenID relies on the Diffie-Hellman (DH) algorithm. DH must be employed to agree on a share secret key used to create the hash of the messages. Unfortunately, as Tsyrklevich and Tsyrklevich (2007) underlines, DH is vulnerable to the man-in-the-middle attacks. The user can thus be phished without noticing it (Hodges, 2009).

The authentication of the different actors: The authentication of the different actors is based on the domain names system (DNS). OpenID only relies on this latter to guarantee someone's identity. Consequently, OpenID is extremely vulnerable to attacks against the DNS. As Laurie (2008) explains, this fact makes the protocol particularly exposed to pharming by cache poisoning.

The OpenID protocol: The OpenID protocol is relatively simple to implement, as long as no extra features are required. This is due to the specificity of this protocol that mainly aims to allow WebSSO. According to Hodges (2009), an identity or a service provider can hardly add new quality features or tailor OpenID in order to make it fit specific requirements. In other words security features can not be added by the identity and service providers. He underlines that OpenID should not work for business concerns that would not conform them to the "trust and accept all comers" philosophy that grounds OpenID. He argues that these companies would not have the possibility to avoid "supporting insecure interactions with just any site and/or user agent". Furthermore, as described in the section 2.5.7, some steps of the OpenID Single Sign-On procedure present some security issues, as we will explain in the next lines.

The OP/IDP discovery is the process that allows a service provider to discover the users' identity provider. The service provider must download the user's URL and extract the address of their identity provider. This procedure increase the vulnerability of the protocol because this is done over insecure networks, from none trustworthy hosts. Several pernicious actions can be undertaken, like downloading all kind of malicious programs that could allow pharming. For example, by changing the address of the users' OpenID and redirect them to a counterfeit identity provider. Actually, this modus operandi opens the doors to all techniques of pharming.

Finally, the fourth step consists in a redirection of the users to their identity providers (Tsyrklevich & Tsyrklevich, 2007). This step makes OpenID vulnerable to phishing. Laurie (2007) explains how OpenID facilitates the task for the eventual fishers who can set up, according to him, “fake providers” that can redirect the users to a fake identity provider and then phish their credentials.

The quality of the credentials: Regarding strong authentication, Recordon and Jones (2008) observe that the identity provider “SHOULD attempt to satisfy the authentication policies requested by the RP”. In addition, they may inform the RP regarding the authentication level of trustworthiness employed. This should be achieved using the four levels of insurance provided by Burr, Dodson and Polk (2006). As a matter of fact, the lack of control renders these recommendations pointless. The conclusion is that strong authentication can’t be implemented efficiently using OpenID. Otherwise, OpenID uses opaque identifiers.

Prevention against social engineering: OpenID has no requirements regarding this attack.

Explicitly, the only requirement of OpenID concerns the protection of the integrity of information using DH. Otherwise the deployment of the different security features is optional for both the identity and the service providers.

5.2.2 Extra protocol security

This subsection concerns the security of the identity and the service providers’ infrastructures. OpenID does not require any security guarantee from either. Neither their infrastructures, nor their identity, trustfulness, goals are checked before their admittance as identity or service providers. Recordon and Fitzpatrick (2006) explain that no central organization controls the users, the identity provider and the service providers. In other words, there is no particular trust relationships based on agreements between the different members. Whoever can become an identity provider and whatever service provider can be allowed to accept OpenIDs.

OpenID gives, nevertheless, some recommendations regarding security. For example, “provisioning of phishing-resistant and other credentials stronger than shared secrets should be accomplished using methods that are at least as strong as the credential being provisioned” (Recordon & Jones, 2008). Furthermore, no audits or controls on the behalf of the OpenID foundation are required. Those facts render the members that do not deploy the security countermeasures and consequently the whole system, particularly vulnerable to the attacks.

Concerning the users, anybody can create one or several Open identities. The choice of the identity providers is free. Users are nevertheless encouraged to “Choose a provider who can secure the log-in process” (OpenID explained, n.d.). The same source provides a list of providers and compares them regarding miscellaneous aspects including security. For the record, some websites that are presented do not even meet any basic security requirements according to authors.

It can be deduced that OpenID does not provide an efficient framework in order to prevent the different attacks. On the contrary it creates a system where some actors (identity or service providers) can be created and then used as tools by hackers. That jeopardizes the whole system.

In the next section, we will, first, expose the strengths and weaknesses of both frameworks to resist to the attacks studied in this work. Then, thanks to this exposé, we will deduce and compare the strengths and weaknesses of both frameworks to protect the confidentiality, integrity and availability of the users’ information.

5.3 Analysis

The analysis of the diverse documents showed that OpenID and LA have two different approaches regarding the prevention of the attacks studied in this work. As a result, both frameworks does not offer the same level of protection against harmful and common attacks like pharming, phishing, social engineering, online password guessing and credential sniffing. As a matter of fact, these attacks jeopardize, at different levels, the confidentiality, integrity and availability of the users' information of a system under attack. Thus, the analysis of the strong and weak points of both frameworks to resist to these attacks will allow us to deduce their strengths and weaknesses to protect the confidentiality, integrity and availability of the users' information.

First, we are going to review the strengths and weaknesses of LA and OpenID to resist to the attacks. Then we will conclude on their strengths and weaknesses to protect the confidentiality, integrity and availability of the users' information.

5.3.1 The strengths of LA to prevent the attacks

As we explained previously, security is central and integrated into LA's framework. As a result, LA provides many security tools to its members but also constraints them to implement the indispensable countermeasures against the attacks. The security groups, the guidelines and best practices that LA provides to its members are valuable. Actually, these diverse elements encourage and help them to implement efficient countermeasures. They give them information about the threats, and provide them some means to improve and update their policies as well as the security of their infrastructures. Hence, LA provides knowledge regarding the non-technological solutions that are necessary in order to deploy safe identity solutions.

As explained, the members need to secure their own environment to prevent attacks like pharming. A federation is considered in its whole by LA. Therefore, the certification and accreditation guarantee that a federation and its members have implemented the required countermeasures and features. The certifications of the members, as well as the audits that are performed on the behalf of LA are two important tools that allow LA to maintain a required level of security.

SAML, the technology utilised for the exchange of authentication and authorisation data between the partners increase the security of the framework.

The service providers within a federation can chose the authentication method. Additionally, they can trust the information coming from the identity providers, regarding the authentication method used and its strength.

Another strong point of LA is that the origin of all messages can be determined. That is, the source of the authentication requests can be established as well as the source of the authorization assertions. Therefore, the origin of an attack can be found allowing the set up of more efficient defences.

Furthermore, LA has implemented an authorization feature that limits the information that is available when the users use their federate credentials to sign-on. This feature reduces the damages caused by successful attacks on the federate accounts.

5.3.2 The weaknesses of LA to prevent the attacks

LA presents a weakness, in the fact that only the federations that have a level 4 certification implement the countermeasure at a maximal level: the federations have a level 1 certification are vulnerable to attacks like pharming. On the other hand, federations that handle sensitive information must detain a level 4 certification.

Finally, no system can be totally secure, irrespective of the countermeasures that are implemented. Unfortunately, hackers find continuously new vulnerabilities, methods or tools to carry out the attacks explored in this work.

5.3.3 The strengths OpenID to prevent the attacks

A strong point of OpenID is that some identity provider implements the countermeasures in order to attract more users. OpenID exposes the security features of some identity providers on its webpage in order to help them.

5.3.4 The weaknesses of OpenID to prevent the attacks

The main weakness of OpenID is its philosophy about the security. OpenID just recommends the implementation of the countermeasures and does not perform any control. This fact renders OpenID vulnerable to all the attacks, especially to phishing and pharming.

Besides, OpenID is not homogeneously protected against the attacks. The members that implement all the countermeasures are endangered by the ones that do not. Regarding, the policies, OpenID does not provide any guidelines to its members.

Another weakness of OpenID is due to the fact that the service providers can't choose and impose the method of authentication. They may be notified about the technique used by the identity providers but with no guarantee about the exactitude of this information.

LA presents some strong points to prevent the attacks while OpenID seems to be vulnerable to all the attacks. In the next subsection, we are going to explore how theses findings influence the protection of the confidentiality, integrity and availability of the users' information.

5.3.5 The protection of the users' information

The description of the attacks showed that the confidentiality, integrity and availability of the users' information were endangered by their success. In this subsection, we will explore what are the strengths and the weaknesses of LA and OpenID to protect the confidentiality, integrity and availability the users' information.

The confidentiality

Thanks to its security requirement, LA offers at least, a basic protection against the attacks. As we explained, the federation and its members must be certified by the IAEG. A level 1 certification offers a minimum prevention against the attacks. A level 4 offers the best protection possible. As a result, this framework is equipped to protect the confidentiality of the users' information depending on the sensitivity of the data. On the other hand, OpenID is not really capable to protect it because of its weaknesses. These weak points are mainly the lack of security requirements and the lack of control over the members vis-à-vis the countermeasures that they implement or not.

LA's authorization feature protects the confidentiality of the information not accessible through single sign-on when attacks against the federate account are successful. This feature does not exist in OpenID.

The availability

Thanks to the security requirement of this framework, LA is well equipped to guarantee the availability of the users' information. On the other hand, OpenID's weaknesses regarding security make it not capable to guarantee the availability of the users' information.

Besides, even when federate credentials are exposed, the users can still log-in using their service provider credentials. In addition, the scope of the OpenID's identities is wider than the LA's ones. Potentially more information remains unavailable. When an OpenID credential is compromised, the availability of the users' information accessible thanks to it is no more guaranteed.

Finally, LA's authorization feature limits the availability of information that it protects, when the users' federate account is not under attack. On the other hand, when these accounts are compromised, the availability of the protected information remains assured thought direct log-in to the service providers.

The integrity

The weakness of OpenID, to prevent the attacks, threatens the integrity of the users' information. On the other side, LA can guarantee it thanks to the diverse countermeasures that have to be implemented by the members.

As we saw regarding OpenID, the means used in order to protect the integrity of the authentication message is not efficient. As explained, DH is subject to the man-of-the middle-attack.

In addition, the LA's authorization feature prevents the protected information from being tempered when the federate account is compromised.

6 Conclusion

LA and OpenID have two different approaches concerning security. LA aims to create a WebSSO framework as secure as possible. This objective is backed by an imposing infrastructure that provides different means to the member in order to inform and help them to resist to various attacks.

The framework that LA provides to its members encompasses guidelines, best practices, policy, security requirements, certifications and audits. These certifications and audits oblige the members to implement the necessary countermeasures. Unlike OpenID, all the members of a federation must implement the required countermeasures.

OpenID does not perform any control of its members and just recommends the implementation of basic security countermeasures. OpenID trust and rely on its members to implement them. This last point constitutes the main weakness of OpenID in its ability to prevent diverse attacks. As a result, OpenID is vulnerable to all the attacks that we studied in this work. Consequently, the confidentiality, integrity and availability of the user's information are weakly guaranteed by this framework.

Finally, LA has another strong point due to its federated nature. A successful attack does not automatically compromise the confidentiality, integrity and availability of a user's information within the whole domain as for OpenID.

We haven't found any strong point regarding OpenID ability to protect the confidentiality, integrity and availability of a user's information. On the other hand, LA has no weakness that OpenID doesn't have, in that matter.

7 Discussion

As discussed previously, OpenID and LA present two different solutions to the same problems: password fatigue and the security breaches it creates. While LA has security in focus, OpenID privileges the ease-of-use to the detriment of security. The result of this comparison is partly based on Hodges' whitepaper (2009). Our work can be seen as a complement of Hodges' one and confirms the potential weaknesses regarding the security of the OpenID protocol.

The results show clearly that OpenID should not be used by websites that manage sensitive information or that are of major interest for hackers. On the other hand, the same results show that LA can't be implemented on every websites as the requirements may be too important for small service providers.

The conclusions presented in this work are alarming regarding OpenID. Nevertheless, OpenID is backed by important companies and is more and more implemented by websites. Different reasons can explain that fact. On the first hand, the results are not valid because the method employed is not valid. As a result, the analysis, which is based, mainly, on the assumption that the lack of requirements and controls imply that the whole OpenID framework presents the weaknesses depicted in this work, could be contested.

Another explanation can be that OpenID has no equivalent on the market and responds to a real demand from the different actors of the web. In other words, its weaknesses regarding security are counterbalanced by its advantages. In the latter case, it appears that the security issues of this framework, that some authors like Laurie (2007) calls "The phishing even" will have to be solved.

8 Future works

The results are indirectly based on the assumption that the countermeasures protect the users' account and information efficiently, on the fact that the countermeasures are really implemented regarding LA as well as on the study of diverse documents regarding the security of both frameworks. This gave actually trustworthy indications about the protection the confidentiality, integrity and availability of a user's information by the frameworks.

On the other hand, the service providers as well as the identity providers need to implement the required countermeasures regardless if they use OpenID or not. A study, could be done, observing, the strengths and the weaknesses of the frameworks, facing the same real conditions. That would allow one to have a real understanding of the advantages and drawbacks of both frameworks regarding the security of the confidentiality, integrity and availability of a user's information.

References

Bailey, M., Orgill, G., Orgill, P. & Romney, G. (2004) *The Urgency for Effective User Privacy-Education to Counter Social Engineering Attacks on Secure Computer Systems*. Proceedings of the 5th Conference on Information Technology Education. October 28–30, 2004, Salt Lake City, UT, USA.

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008) *Thesis projects: a guide for students in computer science and information systems* (2nd version). London: Springer Verlag.

Burr, W., Dodson, D. & Polk, W. (2006) *Information security* National Institute of Standards and Technology, Gaithersburg. MD, USA Available: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf [10 April 2010].

Champagne, D. & Thompson, P. (eds). (2004) *Liberty ID-FF Implementation Guidelines Version: 1.2*. Available: http://projectliberty.org/liberty/content/download/322/2378/file/liberty-idff-guidelines-v1.2.pdf [20 April 2010].

Colomer, M., Garcia Polo S., Medina, M. & Poorter, A. (2006). *Fidelity: Federated identity Management Security based on Liberty Alliance on European Ambit* (p. *161-167).* Highlights of the Information Security Solutions Europe 2006 Conference, 10-12 October 2006, Rome, Italy.

CPNI Centre for the Protection of National Infrastructure (2010) *Phishing and Pharming: A guide to understand and managing the risks*. Available: http://www.cpni.gov.uk/Docs/Phishing__pharming_guide.pdf [20 April 2010].

Cutler R. (eds) .(2008).*Liberty Identity Assurance Framework Version: 1.1* Available: http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf. [20 April 2010].

D'Costa-Alphonso, M. & Lane, M. (2010). The Adoption of Single Sign-On and Multifactor Authentication in Organisations – A Critical Evaluation Using TOE Framework Issues in Informing. *Science and Information Technology, 7*, 161-189.

De Clercq, J. (2002). Single sign-on architectures. *Infrastructure Security,* 2437, 40-58.

Duserick, W. & Fidelity Investments. (eds).(2004*) Liberty Whitepaper on Liberty Protocol and Identity* . Available: http://www.projectliberty.org/liberty/content/download/389/2726/file/Liberty_Identity_Theft_Whitepaper.pdf. [20 April 2010].

Hirsch, F., Philpott, R., & Maler, E. (eds). (2005). *Security and Privacy Considerations for the OASIS Security Markup Language (SAML) V2.0.* Available: http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf. [07 May 2010].

Hodges, J. (2009) *Technical Comparison: OpenID and SAML*. Available: http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html. [07 May 2010].

Jøsang, A., Fabre, J., Hay, B., Dalziel, J. & Pope, S. (2005), *Trust Requirements in Identity Management.* Proceedings of the Australasian Information Security Workshop (AISW'05), January-February, 2005, Newcastle, Australia.

King T. (2006) *Packet Sniffing In a Switched Environment GSEC Practical v1.4, Option 1*. Available: http://www.sans.org/reading_room/whitepapers/networkdevs/packet-sniffing-switched-environment_244. [20 April 2010].

Landau, S. (eds). (2003). *Liberty ID-WSF Security and Privacy Overview Version: 1.0.* Available: http://labs.oracle.com/people/slandau/liberty-idwsf-security-privacy-overview-v1.0.pdf [20 July 2010].

Laurie, B. 19 January 2007. OpenID: Phishing Heaven Available: http://www.links.org/?p=187. [2 April 2010].

Laurie, B. 08-AUG-2008. Security Advisory (CVE-2008-3280). Available: http://www.links.org/files/openid-advisory.txt. . [2 April 2010].

Liberty Alliance project (2005) *Liberty Alliance Whitepaper: Identity Theft Primer*. Available: http://www.projectliberty.org/liberty/content/download/376/2687/file/id_Theft_Primer_Final.pdf [20 April 2010].

Liberty Alliance Project (2010 a.). *Liberty Specs Tutorial.* Available: http://www.projectliberty.org/liberty/content/download/423/2832/file/tutorialv2.pdf_v2_9.pdf. [20 April 2010].

Liberty Alliance project (2010 b). About. Available: http://www.projectliberty.org/liberty/adoption/?f=liberty/adoption [20 April 2010].

Liberty Alliance Project (n.d) *General FAQ*
Available: http://projectliberty.org/liberty/about/general_faq/ [20 April 2010].

Lewis, K. & Lewis, J. (2009) Web Single Sign-On Authentication using SAML. *International Journal of Computer Science Issues,* 2, 41-48.

Madsen, P., Koga, Y. & Takahashi, K. (2005) *Federated identity management for protecting users from ID thef*. Proceedings of the 2005 workshop on Digital identity management, November 11, 2005, Fairfax, Virginia, USA.

Organisation for the Advancement of Structured Information Standards (2005). *SAML v. 2.0 executive overview.* Available: http://www.oasis-open.org /committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf [20 April 2010].

O'Neil, M., Hallam-Baker, P., Cann, S.M., Shema, M., Simon, E., Watters P. A., & White, A. (2003) *Web Services Security.* USA: McGraw-Hill

OpenID explained. (n. d.). Available: http://openidexplained.com [24 April 2010].

OpenID Foundation (2010) Available: http://openid.net/ [20 April 2010].

Pinkas, B. & Sander, T. (2002) *Securing Passwords Against Dictionary Attacks* (p. 161–170). Proceedings of the 9th ACM conference on Computer and communications security, November 18–22, 2002, Washington, DC, USA.

Recordon, D (2007). *OpenID Authentication 2.0 – Final.* Available: http://openid.net/specs/openid-authentication-2_0.html#sign_algos. [2 April 2010].

Recordon, D.& Fitzpatrick, B. (2006) *OpenID Provider Authentication Policy Extension 1.0.* Available: http://openid.net/specs/openid-authentication-1_1.html#anchor30. [6 April 2010].

Recordon, D.& Jones, M. (2008) *OpenID Provider Authentication Policy Extension 1.0*. Available: http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html#anchor10 [7 April 2010].

Renaud, K. (2007) A process for supporting risk-aware web authentication mechanism choice. *Reliability Engineering and System Safety, 92,* 1204–1217.

SANS Institute (2006*) Password Policy.* Available: http://www.sans.org/security-resources/policies/Password_Policy.pdf [27 June 2010].

Sheckler, V. & Varney, C. (eds). (2005) *Deployment Guidelines for Policy Decision Makers Version 2.9.* Liberty Alliance Projet. Available: http://www.projectliberty.org/liberty/content/download/373/2678/file/deployment_guidelines_v2_9.pdf. [20 April 2010].

Srivastava, T. (2007). *Phishing and Pharming – The Deadly Duo*. SANS Institute. Available: www.sans.org/reading_room/whitepapers/privacy/phishing-pharming-evil-twins_1731. [20 April 2010].

Smith, D. (2008). The challenge of federated identity management. *Network Security,* 4, 7-9.

Suess, J. and Morooney, K., (2009). Identity Management and Trust Services: Foundations for Cloud Computing. *EDUCAUSE Review,* 44 (5), 24–43.

Talbot, D. (2006). Universal Authentication. *Technology Review*, 109(1), 65-66.

Tsyrklevich, E. & Tsyrklevich, V. (2007) *Single Sign-On for Internet: A Security Story*. BlackHat, USA. Available: https://www.blackhat.com/presentations/bh-usa-07/Tsyrklevich/Whitepaper/bh-usa-07-tsyrklevich-WP.pdf [20 April 2010].

Uberti, J. (eds). (2005). *Liberty ID-SIS Presence Service Implementation Guidelines Version: 1.0-12*. Available: http://projectliberty.org/liberty/content/download/1053/7221/file/draft-liberty-id-sis-presence-guidelines-v1.0-12.pdf. [20 April 2010].

de Vivo, G., de Vivo, M.& Isern, G. (1998). Internet security attacks at the basic levels, *ACM SIGOPS Operating Systems Review*, 32(2), 4-15.

Wood, P. (2005). Implementing identity management security-an ethical hacker's view. *Network Security*, 9, 12-15.