InCommon

MICHAEL SMITH[1]

[1] *School of Informatics and Computing, Bloomington, IN 47408, U.S.A.*
[*] *Corresponding authors: mls35@iu.edu*

paper2, April 4, 2017

InCommon is a federated security service that is responsible for the management of identity verification solutions serving U.S. education and research[1]. All users within this federation allow partners to share identity information in order easily recognize the user. This federation provides numerous benefits for users and service providers through the convenience of single sign on capabilities for the user. Privacy is enhanced by limiting the distribution of personal information amongst numerous service providers. Scalability is easily facilitated due to the unified policies and management procedures. InCommon utilizes the single sign on software Shibboleth which is an open source project that enables federated organizations to connect users to various applications through a convenient secure method. The backbone of this software is built on the language SAML or security assertion markup language that creates the basis for its application. Programs such as InCommon assurance and university case studies are examined.

Keywords: InCommon, User authentication, identity management, I524

ttps://github.com/cloudmesh/sp17-i524/blob/master/paper2/S17-IO-3019/report.pdf

This review document is provided for you to achieve your best. We have listed a number of obvious opportunities for improvement. When improving it, please keep this copy untouched and instead focus on improving report.tex. The review does not include all possible improvement suggestions and for each comment you may want to check if it applies elsewhere in the document.

The reference in the abstract should be moved to the main text. References in the abstract are ok in general, but should be reserved for specific claims that critical to the abstract and paper, e.g. "In this paper, we reproduce the findings that ... [1]..." In your case, the reference is general and should be included in the main text.

Some parts of the abstract, such as the sentences on using Shibboleth and SAML don't seem that critical and can be omitted. The abstract should tell the reader what is most important about the technology and entice them to read the entire paper, and going into these two details in this case might not be necessary. Leaving up to you whether to omit. Good abstract overall.

Overall, great job. You can improve the flow of the paper by providing more transition between some of the sections. In addition, a couple sections are borderline out of scope for a neutral paper like this. Finally, there are some cases where you can use more neutral language. See below for details.

Assessment: Some revisions suggested.

INTRODUCTION

Electronic credentialing of individuals requires an effective implementation of a set of policies and procedures. In order to be successful, identity management requires an organization to keep user information up to date, providing the trust needed for secure transactions, and determine user access of online applications. The major issues with identity management is the increasing number of cloud services or applications that are web hosted

,

all of which have different policies for implementing identity verification. The solution is to establish a federation which is defined

as

"an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transaction" [1]. Within this federation the parties come into an accordance on the policies associated with identity management. A great example of a federation that encompasses this definition is InCommon

.

INCOMMON

InCommon was founded by the advanced technology organization Internet2. Their mission is to create an environment that facilitates the ability for educators and researchers to collaborate regardless of their location. Their network encompasses over 90,000 institutions, 305 universities, 70 government agencies with network operations center powered by Indiana University [2]

Through the InCommon service, users will no longer have to

Why "will no longer?" Isn't this already the case?

remember a plethora of usernames and passwords for each web service. Instead

,

they will be able to have single sign on (SSO) conveniences. Giving time back to faculty, staff and students for education, research and other contributions to the University. Any service provider within this federation no longer needs to manage databases of username and passwords, the users are verified and then administered security tokens to then engage with service providers within the federation. By limiting the amount of identity information required of the service provider, the users privacy is safe

Probably more correct to say "safer" since there is still (always) risk. But storing login information in a single place is definitely an improvement.

in the event of a security breach of the service provider.

SAML

The language used by InCommon is referred to as security assertion markup language or SAML. This language is based in XML which allows for the exchange of authentication information between a user and a provider [3]. It is the industry accepted standard language for identity verification by government, businesses and service providers.

Could you provide a source or more detail about it being "the industry accepted?"

The general user verification is done by an identity provider(IdP) which is responsible for user authentication through the use of security tokens with SAML 2.0 [4]. Service providers (SP) are defined as entities that provide web services, internet, web storage etc. They rely on the IDPs for the verification process. A significant amount of the major web service providers such as Google, Facebook, Yahoo, Microsoft, and Paypal play a dual role and exist also as identity providers.

SHIBBOLETH

Shibboleth is the service that has a suite of products that assist the InCommon federation through utilization of SAML in programming languages such as C ++ and Java[5]. The normal authentication process for Shibboleth is to intercept access to a service, determine who is the identity provider for the user. Once the identity provider has been discovered a SAML authentication request is sent to the identity provider. Identity providers SAML response will have the relevant user information for verification. The extracted user information will then be passed to the service provider or resource determining user accessibility. While the process sounds complex it will occur instantaneously, after the user has entered its single sign on.

CERTIFICATE SERVICE

The types of certificates that InCommon have available for issue are SSL/TLS, extended validation, client, code signing, IGTF server, and elliptical curve cryptography certificates (ECC). SSL (secure sockets layer) is "the standard security technology for establishing an encrypted link between a web server and a browser. The link ensures all data is passed between the web server and browers remain private and integral"[6]. The details of an SSL certificate issued by InCommon will contain user information and the expiration date. For all educational institutions, InCommon offers unlimited server and client certificates for the annual fee.

DUO

In collaboration with the trusted access company Duo, Incommon offers two factor authentication through the utilization of the users smart phone[7]. A duo mobile app supports the following platforms: Apple iOS, Google Android, Windows mobile, Palm WeboS, Symbian OS, RIM blackberry, Java J2ME. The application will generate a randomly generated one time password that the user will type into the web application for a more secure identity verification. Two factor authentication does not require smartphone, other methods such as automate voice calls or SMS messages. In addition to Duo mobile, a service called Duo push is available which does not require the user to type in the password, authentication occurs directly from the mobile app. It is up to the university to determine how Duo is deployed, whether it will occur with the identity provider or the service provider. If it is deployed at the service provider destination, Duo web supports the following client libraries: python, ruby, classic ASP, ASP.net, Java, PHP, Node.js, ColdFusion, and Perl.

The content for these sections (SAML, Shibboleth, Certs, Duo) is good and at the right level of detail. However, there is not much flow between the sections. You can improve by putting these four as subsections to an Architecture section and provide some motivation for why each component is necessary and how they fit together. E.g. "Architecture: InCommon's main functionality is implemented by SAML. <SAML subsection>. Then: To facilitate InCommon's use in programming environments, <Shibolleth section>" and so on. Just provide a little more transition and motivation for why each part of the system exists.

ASSURANCE PROGRAM

Incommon offers an assurance program that will examine and the practices of an organization and will rank them based on a number of criteria. Areas of examination include "...identity proofing(such as checking government issued ID before accepting that people are who they say they are), password handling (including making sure that passwords are not sent or stored in the clear), and authentication(such as ensuring the resistance of an authentication method to session hijacking)" [8]. There are two levels of assurance in the InCommon program, bronze and silver. Bronze is comparable to NIST level of Assurance 1

What is that? You haven't mentioned it in the paper before.

, which is for common usage of internet identity management. Silver is comparable to NIST level of Assurance 2, which defines the institute as having sufficent requirements provide a security at the level for a financial transaction [9]. Compliance with

a bronze level only requires a level of self certification of the requirements, where as a silver level is more difficult to achieve. A third party or evaluator that has been verified by InCommon is required to peform an audit ensuring the identity provider is meeting all the rules and requirements. Many organizations and government agencies such as a national institute of health and public universities are requiring identity providers to become certified in this program.

You may want to start this section with this last statement about large agencies requiring this kind of certification. Otherwise it sounds like you're describing a service that is outside the scope of the paper.

COST

The current rate for Universities to subscribe to the InCommon service varies based on a couple of factors such as highest level of degree offered (Doctoral, master's etc.) and Carnegie classification. The range in price will vary from 20,000 to 2,000 dollars annually [10]. If the organization is an internet2 member, a 25 percent discount applied to the annual fee.

This is out of scope for the paper. Focus on the service being provided and how it is implemented, and how it compares to similar service. Interested readers can figure out how cost themselves.

UNIVERSITY OF MINNESOTA

Please, give more context and a transition from the previous sections of the paper. E.g. "One example where InCommon was successfully deployed is..."

The University of Minnesota adopted into the InCommon federation on September 2010 [11]. The university contains 51,000 students, and over 300 institutes. Their previous identity management vendor charged on a per certificate basis. This differs from InCommon which offers an annual fee with unlimited certificates. This simplifies the ability for IT departments within Universities to properly budget. Additionally the university saw a tremendous

"tremendous" is subjective, please avoid

cost savings of 38,000 dollars. This model also encourages enhancing security because cost does not influence which servers to secure.

STUDENTS ONLY

The bottom line of a university is not the only one who sees the cost benefits of InCommon [12]. Student verification provider known as students only is a way for students to enroll to verify their status as a student. This verification is then passed to businesses that would like to offer discounts to students. To prevent nonstudents from taking advantage of generous

"generous" is subjective and more appropriate for an advertisment; please avoid.

offerings of companies it can be cumbersome for a student to properly verify their status. With the help of InCommon Students Only helped streamline the process for students to verify their identity in a single sign on. This reassured the companies and students were able to save money without the difficulties of personally handling identity verification.

Like the Cost section, this is bordeline out of scope, and sounds a bit like a marketing pitch. Consider skipping unless you can provide some source that more neutrally establishes how something like this is beneficial to students.

CONCLUSION

As the number of services on the web continue to grow it can be quite challenging for both universities and service providers to properly manage accessibility manage identities. InCommon hopes to address this issue by bringing U.S. educational institutes into the same federation. This will create a common groundwork of policies and procedures related to identity management. Through this unity, users such as faculty, staff, and students alike can benefit from the obvious conveniences of single sign on. However, they will also benefit from enhanced security and privacy. Institutions that have entered into InCommon have seen benefits such as cost savings over competitors in this market as well as simplification of the billing process for University IT. The unlimited certificate model as well as the diverse types of certificates allows IT flexibility to issue the appropriate certificate without the worry of budgeting constraints. Partners such as Duo further improve security through two factor authentication dramatically improving the protection of the user.

REFERENCES

[1] InCommon, "Incommon overview," Webpage. [Online]. Available: https://www.incommon.org/docs/presentations/InCommon_Overview.ppt

[2] ——, "What is the incommon federation?" Webpage. [Online]. Available: https://spaces.internet2.edu/download/attachments/2764/final_InCommon.pdf

[3] Wikipedia, "Security assertion markup language," Webpage. [Online]. Available: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[4] empowerID, "Service providers, identity providers & security token services," Webpage. [Online]. Available: https://www2.empowerid.com/learningcenter/technologies/service-identity-providers

[5] Shibboleth, "Shibboleth," Webpage. [Online]. Available: https://shibboleth.net/

[6] SSL, "What is ssl?" Webpage. [Online]. Available: http://info.ssl.com/article.aspx?id=10241

[7] InCommon, "Incommon multifactor," Webpage. [Online]. Available: https://www.incommon.org/duo/

[8] M. Erdos, "An introduction to assurance," Webpage. [Online]. Available: http://iam.harvard.edu/resources/introduction-assurance

[9] InCommon, "The incommon assurance program," Webpage. [Online]. Available: https://www.incommon.org/assurance/

[10] ——, "Certificate service annual fee schedule," Webpage. [Online]. Available: https://www.incommon.org/certificates/cert_fee.html

[11] ——, "The university of minnesota enables security at scale with incommon," Webpage, July 2016. [Online]. Available: https://www.incommon.org/docs/eg/InC-Cert_CaseStudy_Minnesota.pdf

[12] ——, "Incommon flies high with students only," Webpage. [Online]. Available: https://www.incommon.org/docs/eg/InC_CaseStudy_StudentsOnly_2009.pdf