Single Sign On Recommendation for Adams Healthcare

Allison Adams

Seattle Pacific University

ISM6331 Winter 2017

Abstract

The purpose of this paper is to recommend that Adams Healthcare institute a Single Sign On (SSO) Service. Adams Healthcare is a growing healthcare clinic where an employee uses on average fifteen individual applications and services in one day, each with unique usernames and passwords. In the past year Adams Healthcare has seen a 30% growth of calls to the helpdesk surrounding passwords, an impact that is causing both excess budget expenses and employee frustration. The proposed implementation of a SAML Integrated SSO is analyzed through the lens of the CIA Security triangle, taking time to consider the security risks and benefits of the system. Through this exploration it is clear that a Single Sign On implementation will create a homogenized and improved user flow and is a valuable addition to Adams Healthcare.

Keywords: *Single Sign On, SAML, Confidentiality, Integrity, Availability, Healthcare*

Single Sign On Recommendation for Adams Healthcare

Introduction

Presently, the Help Desk at Adams Healthcare reports that 30% of all calls received are regarding password resets and lockouts. The blame cannot be placed on the employees. Company policy dictates employees utilize strong passwords, and with a standard to have a 12-character password that is not written or stored. The employees at Adams Healthcare interact with over fifteen applications in the course of a workday and each application requires a unique password and username.

I recommend Adams Healthcare support Single Sign On (SSO) for their employees to use across intranet programs. Such a system presents a solution that, "allows users to authenticate once to a central server, which then negotiates connections to authorized systems, hosts and applications for that user" (Holloway, 2002). The advised SSO implementation will remove the vulnerability of an employee forgetting authentication requirements as well as provide efficient and comprehensive administration tools for management. Adams Healthcare will also reap a financial benefit from such a system. According to a 2011 study "How Single Sign on is Changing Healthcare" conducted by the Ponemon Institute SSO has proven annual economic efficiencies of up to $2,675 per clinic and 10 minutes a day (Ponemon, 2011). Introducing SSO at Adams Healthcare will provide direct economic gains, and increase employee efficiency in the workplace.

The transition to SSO will undoubtedly reconcile the fragmented sign on process currently in place at Adams Healthcare. Nonetheless, it is critical to evaluate this decision through the lens of the Confidentiality, Integrity and Availability (CIA) Security Triangle before pursuing full implementation. The CIA Triangle provides Adams Healthcare with a baseline view and understanding of the security effectiveness of SSO (Whitman & Herbert, 2016, p. 10 - 11). The confidentiality of the data must be secure, requiring Adams Healthcare to effectively authorize and authenticate users. This means that the proper security procedures must be in place for secure data storage and transfer. Secondly, Adams Healthcare must establish an architecture that provides and protects data integrity. Data that maintains its integrity is authentic and ensures that Adams Healthcare can complete core business functionality. Availability, the final pillar of the CIA Security Triangle, is critical to the success of an SSO implementation. In order to support a profitable and working business model Adams Healthcare must work to establish a system that provides both sign on and reporting capabilities, even in the face of malicious activities. With this perspective in mind Adams Healthcare can lay the framework for a successful SSO implementation.

Confidentiality

Confidentiality, or privacy, of data is the foundation for application security. Information confidentiality "ensures that only users with the rights and privileges to access information are able to do so" (Whitman & Herbert, 2016, p. 15). The security required to support SSO is twofold. First, Adams Healthcare must provide security for this authentication process through a Security Assertion Markup Language (SAML) integration. SAML protocol is a data format for communication between networks ("Dev Overview of SAML", n.d). When employees first attempt to log on into the SSO system they are instructed to enter their username and password. After entering these authentication details a generated SAML protocol message is sent to the identity provider. Then, "the identity provider site asserts to the service provider site that the user is known to it and provides the user's name and possibly additional session attributes.” (Ragouzis et al. 2008) For example, the additional session attributes for Adams Healthcare will include access levels for varying employees including nurse, physician or physician assistant. The SSO is not a password synchronization. The SSO implementation will allow employees to retain individual passwords for applications, but offer a method for simultaneous log in through a unified system. My recommendation is that we move forward with a two factor authentication process in tandem with the SAML SSO implementation. This combination of something our employees have, and something that our employees know decreases the risk of security breaches through malicious activity (Kelly, 2002).

Secondly, Adams Healthcare must address the concerns surrounding access controls and data privacy. Adams Healthcare has several disparate databases that contain access and authentication information from different systems. As a result, monitoring and managing access controls for each system is cumbersome and unreliable. Transitioning to the SSO architecture will provide a role based discretionary access control model that is, “focused on the permission or privileges that a subject has on an object, including if a subject may access an object and how the subject may use that object” (Whitman & Herbert, 2016, p. 299). Through SSO Adams Healthcare will realize the benefit of a single, centralized database for employee credentials. The central database will serve up passwords for each subsequent application that the employee interacts with throughout their work day.

In accordance with the Access Control Matrix created by management, the centralized database increases the ease of assigning employees to user groups. This organizational matrix list assets and employees with corresponding data confidentiality levels (Whitman & Herbert, 2016,

p. 657). Concerning the healthcare industry, there are several federal compliance regulations that Adams Healthcare must enforce. Most notably Adams Healthcare must ensure that the SSO implementation retains full Health Insurance Portability and Accountability Act (HIPPA) compliance. Through the creation of an Access Control Matrix leadership can make informed decisions assigning employee's read/write credentials for each specified system.

Integrity

Integrity is the second facet of the CIA triangle. Data integrity for the support of the SSO ensures that information needed for SSO is not, "exposed to corruption, damage, destruction or other disruption of its authentic state" (Whitman & Herbert, 2016, p. 16). This means that several "confidentiality protection mechanisms" (Nataraja,2012) must be installed and configured to certify that the data is secure both at rest and in motion during the SSO lifecycle. Digital signatures that exist in SAML protocol messaging preserves this data integrity. An additional measure is through, "RSA encryption with the public key available in all your client apps but the private key only available on the auth server(s)." (Aimonetti, 2012) By ensuring that the data stored in our centralized database is not tampered with by malicious attacks Adams Healthcare is able to confidently use the SSO on all systems within the health care center.

The ability for reliable data audits is a core aspect of data integrity and accountability. With all records of system access stored in one place the reporting and auditing processes become streamlined and more efficient and allows for more detailed identity management. Leadership will have the ability view all employees and their session IDs for each application and monitor that the correct employees have access to the correct applications. The history allows for the determination of, "not only which accounts were breached, but also what was done during the breach and from where the breach took place, creating an effective audit trail" (Uzialko, 2017). The SSO application will consolidate this history into system logs, providing a concise history of all application logins, both successful and failed attempts.

Availability

The final pillar of the CIA triad is the availability and the accessibility of the system. The applications must remain available for all our employees when they are required, or risk blocking critical core business activities. This means that the SSO integration shall "enable authorized users - people or computer systems- to access information without interference or obstruction and receive it in the required format" (Whitman & Herbert, 2016, p. 12). Due to the nature of SSO access it is vulnerable to a denial-of-service attacks that will remove employee access from all, not just one, application. Additionally, SSO with the proposed SAML integration is susceptible to XML Parsing. To mitigate these risks, and ensure system availability to our employees Adams Healthcare must follow strict security protocols. Adams Healthcare adheres to these protocols through the validation of both the XML Schema and the digital keys, and removing the automatic download of schemas from third parties (Krawczyk, n.d).

A computer left unattended will be logged into all systems, allowing for increased access when accessed by a malicious user. To combat this problem, it is essential to have strict and enforceable password lockout procedures. This means that there are set timeframes that the SSO system will require an employee to re-enter the information needed through two factor authentication. Additionally, it is important that when an employee logs out, the SSO consequently will remove that specific employee's access to all systems and applications. As explained by Pathberiya (2013), the SAML implementation for SSO this process is very similar to how a login request is created. A log-out request is then validated by the identity provider. He continues that once the request is validated and a log-out response generated, the SSO session is ended for that specific employee. Subsequently, this log-out response logs the employee out of all systems, eliminating the risk of a lingering log in and an exposed vulnerability to the company.

To prepare for these malicious attacks Adams Healthcare must fully document and assess all the risks associated with the SSO implementation by preparing a Risk Management document as well as a contingency plan as part of Business Continuity Planning. This document will outline the policies, programs and the technologies impacted by SSO. Considering this program will be new for our employees it will be important that there is a heavy piece of education that is associated with the launch. This will involve trainings for all employees with curriculum explaining how the SSO works, and what their responsibilities as an end user of the systems entail. On the grounds that employees will not be required to input multiple passwords Adams Healthcare will be able to increase the requirements for the single password. Instructional information around these new guidelines will be effectively communicated throughout the company.

Conclusion

It will be important to monitor several key performance indicators (KPI) with the implementation of SSO. The first KPI that will be measured is in the number of calls received by the help desk. With the baseline of the current 30% of calls regarding password we can track and analyze the percentage of calls in 2017. The second KPI that can be measured is through employee satisfaction with technology. This past year Adams Healthcare has received several complaints from employees through the Employee Opinion Survey. For the upcoming year we can review the surveys and compare the results to measure the effectiveness of the SSO implementation. Through these measurable KPIs Adams Healthcare can justify the implementation costs with a clear return on investment, and provide a competitive advantage for the company.

Adams Healthcare is ready to provide its employees with a seamless process for access for all intranet systems. Adams Healthcare will see a direct decrease in calls to our Help Desk, reducing overhead IT costs for password resets. Additionally, Adams Healthcare will see a reduction in production costs for supporting several disjointed applications. Through supporting an SSO system employees at Adams Healthcare will be able to focus on providing better services for patients and able to work with technology, instead of against it. The implementation of a Single Sign On Service with SAML integration at Adams Healthcare will make an instantaneous positive contribution, providing employees a single and homogenous method for accessing all core business applications.

Resources

Aimonetti, M. (2012, April). Building and implementing a Single Sign-On solution. In *Merbist*. Retrieved February 25, 2017, from http://merbist.com/2012/04/04/building-and-implementing-a-single-sign-on-solution/

Dev Overview of SAML. (n.d.). In *OneLogin Developers*. Retrieved February 10, 2017, from https://developers.onelogin.com/saml

D. H. (2002). Single Sign-on: Deployment Considerations. GIAC Certifications. Retrieved February 10, 2017, from https://www.giac.org/paper/gsec/1582/single-sign-on-development-considerations/102925.

How Single Sign-On Is Changing Healthcare (2011, June). In *Ponemon Institute*. Retrieved February 12, 2017, from http://www.ponemon.org/local/upload/file/Imprivata_SSO_FINAL_9.pdf

Kelly, M. (2002). Is Single Sign on a Security Risk? *GIAC Certifications*. Retrieved from https://www.giac.org/paper/gsec/811/single-sign-security-risk/101711

Krawczyk, P. (n.d.). Secure SAML validation to prevent XML signature wrapping attacks. In *Open Web Application Security Project (OWASP)*. Retrieved February 15, 2017, from https://arxiv.org/pdf/1401.7483.pdf

Nataraja, V. (2012, December 2). Is SAML An Effective Framework For Secure SSO?. Retrieved February 13, 2017, from http://vinayendra.com/SAML.pdf

Pathberiya, A. (2013, June 28). How SAML2 Single Logout Works. In *xacmlinfo*. Retrieved February 25, 2017, from http://xacmlinfo.org/2013/06/28/how-saml2-single-logout-works/

Ragouzis, Nick, John Hughes, Rob Philpott, Eve Maler, and Paul Madsen. "Security Assertion Markup Language 3 (SAML) V2.0 Technical Overview 4." *Oasis Open*, Oasis, 25 Mar. 2008, docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html. Accessed 22 Feb. 2017.

Uzialko, A. (2017, February 23). Best Single Sign-On Solution for Enterprise Businesses. In *Toms IT Pro*. Retrieved February 25, 2017, from http://www.tomsitpro.com/articles/single-sign-on-solutions,2-853.html

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security* (5th ed) Boston, MA: Cengage Learning.