SAML SSO Design

Patrik Rodný

Abstract:

Software companies are experiencing a persistent business demand for new software projects. Even though a sophisticated software product can utilize its modularity with intention to improve in specific area, every change with higher complexity may cause that the software project lowers its success by exceeding planned time and resources. The situation is no different in the field of economic and juristic applications. The intent of this paper is to mention a description of security solution design to create possibilities for company collaboration, to enhance the identity security and to improve the usability. Within the design phase there is an opportunity to reuse existing and proven standard solutions. The presented example of Security Assertion Markup Language Single Sign-On (SAML SSO) design deals with securing several multidomain web applications with a common user base. Within the design, Spring Security is highlighted for its reinforcement in modularity and strong popularity within Java programmers. Considering different design views using the methodology MMDIS, the SAML SSO design is prescribed to unite the existing software projects with the goal to offer complex, usable, and secure products to customers.

Keywords:

SAML, SSO, Spring, security, MMDIS.

ACM Computing Classification System:

Security and privacy, security services.

Introduction

This paper presents the design of SAML solution as a key to accomplish higher success in comparison to case when complex changes to the existing project cause the software project to exceed expected time and budget. The intent of this paper is to answer a question whether we can utilize the security standard, proven by time, to solve a problem with lack of clients of multiple economic and juristic organizations, as well as to increase the security and usability of the products. Modeling and analysis are combined so that a design substantiation could support the programmers in their future projects. For detailed characteristic of a solution please refer to my bachelor's thesis [5].

The purpose of SAML is to outline a communication between systems offering services (service providers - SP) and trustworthy system (identity provider - IDP) [6]. Trustworthy system is the one on which is the authentication, or alternatively also authorization delegated. IDP must be well secured and trustworthy in providing identities to SP.

The goal of secure design is that minimal information is to be sent, and the identity identifiers always reach their destination unmodified and unrelieved by the attacker. This can be considered as a safe state. By this manner, the attacker could be eliminated from the dangerous communication game. By implementing SAML SSO we secure the sent identity information using a pair of public and private key and reduce the total number of times when the password is sent over the network.

Apart from securing the application, we may also think about usability and user experience. In direction of providing the necessary comfort and easy choices to the application user, we assume that lesser the authentication procedures the user goes through, the more stamina he could utilize while using the application. Security authentication schemes like Single Sign-On or Single Log-Out may be considered also as a tool providing user a relief from unnecessary actions.

1 Situation in Regard to Authentication Mechanism with SAML

Today, many applications step aside from duplicating the stored identity information across multiple systems [5] [6]. A SAML scheme can be used as a special case of SSO, where the participants or parties are operating under different domains create a so-called federation. Special agreements and standards must be applied to the federation so that an access could be granted for a user across multiple simultaneous applications. In case of cloud environment, we can talk about federated groups created to protect identities or user credentials. A standard called Federated Identity Management (FIdM) describes how the identity management information is transferred between domains so that the user party can benefit from the application and its resources without the need to discover the detailed identity of application user [4].

In terms of FIdM, there are three most popular security standards. One of them is SAML. Another standard for delegation authentication is called Open Authentication (OAuth). The last one, OpenID Connect (OIDC) is simply only an identity layer on the top of OAuth 2.0 authentication protocol. These standards use tokens which can also partially represent an encrypted digital identity of application user [4].

In oppose to SAML, the OIDC alternative offers better functionality than it was before. It is simple and easy to implement its specification because the communication is using RESTful APIs. Its target usage is web, cloud, mobile devices and IoT. It is still a developing standard, where for instance Facebook and Twitter are using their own altered versions of OIDC. The next generation authentication protocol requires time for its acceptance in business applications. [4] While in the long run the federated authentication protocol is expected to change from SAML to OIDC. [2]

SAML is a recognized standard as it is being successfully and widely accepted for enterprise business usages. Major international companies such as VMware, IBM, and Google have adopted it successfully. [1] Despite the wide usage we must say that SAML has negatives concerning mobile devices and IoT because of the high XML verbosity compared to JSON. [4] Another thing worth mentioning is that SAML is relatively difficult to implement, configure and maintain as a security solution.

For the current systems there are possible approaches how to support both SAML and OIDC by implementing token translation. There have been more solution proposals introduced in the past. One of the solutions was introduced in 2019. The solution proposal includes 5 main participants [2]:

1. User Agent
2. OIDC Client
3. OIDC Broker
4. SAML Proxy
5. IDP

The goal is that the User Agent is authenticated by SAML IDP while using OIDC standard. The IDP cannot reply to OIDC client with SAML message directly. There is a translation logic between the OIDC identity information format and SAML identity information format. For this purpose, is the OIDC Broker introduced. OIDC Brooker does not connect to identity provider directly, but it utilizes another component called SAML Proxy. SAML Proxy is using HTTP redirects to pass the identity information from IDP to the OIDC Brooker. From the SAML perspective it acts as middle peace (behaves like both - identity provider and the service provider), but it additionally provides multiple microservices like User Consent, Discovery Service, and OIDC Interface. In case of OIDC request, the OIDC interface does the OIDC token to SAML AuthRequest conversion. [2]

Even though the encryption and signing offers good level of protection, weaknesses have been shown on the side of identity providers where the authentication is being performed. [3] SAML SSO can decrease the amount of entered authentication information, however it cannot eliminate the danger of Man-in-the-Middle attack. To improve in this area, it is suggested to utilize Multi-Factor Authentication (MFA) which is usually not a common practice in many IDP implementations because of the fact, it is not a part of Standard Operating Procedures. [3] Multifactor authentication stands from a definition for a combination of something you possess, something that you grasp and something that you constitute. It is the goal of the designer to find the proper ratio between the usability and security of different authentication methods. [3]

Many existing commercial SAML IDPs are ready for deployment and only need to be properly configured. On the site of SP, a programmer can choose from variety of security libraries which can be included into the application. To introduce a specific library, a security library from Spring Security project was chosen. This library was included into the Spring Security project only recently. [5] Even though we can observe an increase in length of the encryption/decryption keys, the long living concepts like RSA keys continue to provide security for exchanged information. The theory remained because efficient approach to break this cryptographic problem is out of actual human knowledge. [5]

The two most known types of attacks to SAML systems are Denial-of-Service (DoS) and Man-In-The-Middle (MITM) Attack. DoS is when the attacker tries to flood IDP with requests from stolen authentication information. MITM is when the sent messages are captured and misused.[4]

The research discussing about how is the SAML testing, and code audit performed, reveals a sad news. The usually used semi-automated code audits of SAML solutions lack efficiency and are less reusable in comparison to sophisticated testing methods. For this purpose, lets mention a testing framework that can deal with it. [1]

There are two different approaches of testing SAML SSO systems [1]:

- a model oriented and
- an implementation oriented.

In case of implementation-oriented style, we consider the specific code implementation and vulnerabilities. This approach has shallow viewpoint in the way that it is difficult to discover vulnerabilities because of the absence of global abstraction. On the other hand, in case of model-oriented style, the system specifications are converted into the state machine. Within the model-oriented approach, we can distinguish 2 models. The first one is responsible for catching sent data during a successful login scenario. Afterwards the second model tries to alter the data while assuming unexpected behavior. The data alternations can include randomly inserting enclosing html element tag or inserting malicious JavaScript or SQL scripts into the message or its header. [1]

The increase in software projects caused the number of application users to rise rapidly. From the usability perspective, the application has special constrains to the passwords which has ongoing negative effects for application user. We can talk about stress to fulfill the security expectations. Single Sign-On (SSO) solutions also provide an ease of application use and improve the user's experience while working with multiple applications. [3]

2 Proof of Concept - SAML Single Sign-On Design

Many companies today take advantage of e-business to improve communications with their customers through sophisticated applications. Each business does its activity to maximize profit, but it must respect the boundaries of laws in the country in which it is performed.

In this research the firms are divided into 2 categories. In the first category there are economic and juristic firms. These firms offer software products for the second category. To the second category they belong for instance companies with focus on civil, mechanical, electrical, chemical engineering or healthcare. The firms in the second group are supposed to be clients of the first group.

The law and economic firms with their software have their own clients which does not necessarily have to be distinct. The firms are speculating on how to be more supportive for a larger user base.

Can we utilize an existing proven solution within the design to solve the problems of enhancing security, improving usability and support the collaboration of juristic and economic firms? We can have a closer look at proving the answer to the hypothesis by modeling an example of SAML solution.

Each company is offering services while having their own database of clients and these databases are not shared in between companies. From this we presume duplicities across different databases.

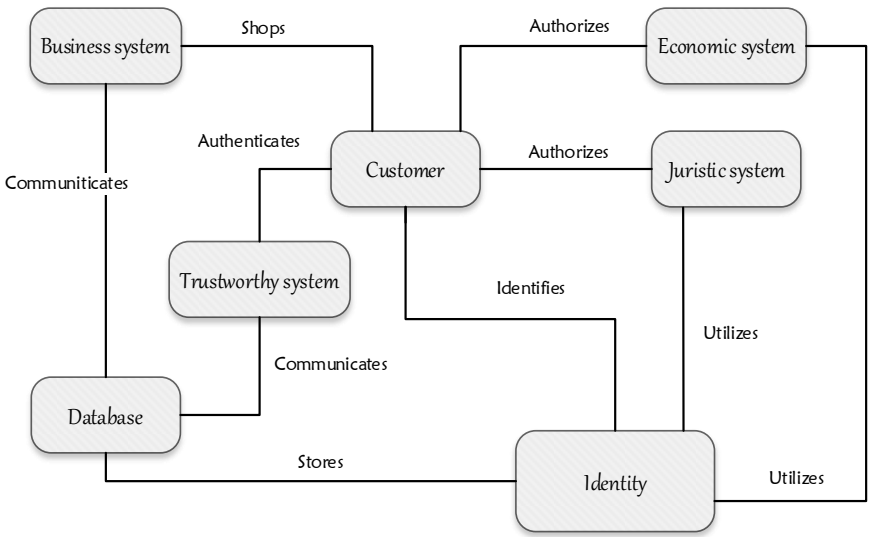

Fig.1. MMDIS Conceptual class model [5]

The design idea is that the economic and juristic firms could create a pact to offer complex products to their customers. We can look at each of software system as if it would be an SP instance. To design SAML standard, two other systems would be trustworthy system (identity provider - IDP) and a business system which would serve as a common gate to selling a license to economic and juristic applications. The cooperation between the systems could be secured by a common database which would store the user identities. [5]

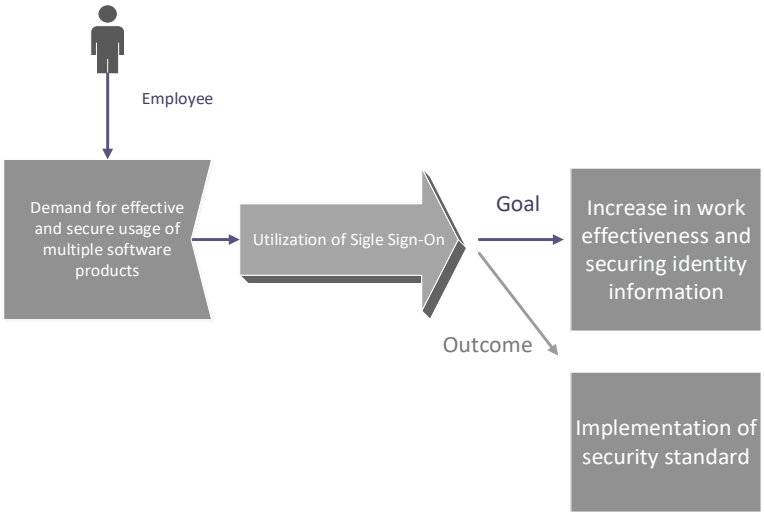

Fig.2. MMDIS Process model [5]

Providing that the budget allows it, there is a possibility to choose from many commercial IDP implementation like Octa or Microsoft ADFS, or to satisfy with open-source alternatives like Shibooleth or Keycloak. [5]

On the side of the service provider, is Spring Framework considered to be a focal point in security solution design. Spring framework is suitable because of the modularity of Spring Security components. So, after the different authentication mechanism are applied, authorization can be effectively handled.

The Spring support for SAML started with an extensions project. [5] The problem with this was a library that utilized a lot of dependencies on which were vulnerabilities discovered. The Spring decided to discontinue the support of the extension library and only recently introduced SAML library in the Spring Security project itself. To get a sense of some discovered vulnerabilities please refer to table below presenting an analysis from 1st of May 2021:

Table 1. Overview of analysis with OWAPS Dependency Checker 6.1.6 for vulnerabilities reported by NIST.

Library (groupId, artifactId, version)	Unique dependencies count	Vulnerable Dependencies	Vulnerabilities Found
org.springframework.security.extensions:spring-security-saml2-core:1.0.0.RELEASE	25	13	49
org.springframework.security.extensions:spring-security-saml2-core:1.0.10.RELEASE	33	10	13
org.springframework.security:spring-security-saml2-service-provider:5.4.6	23	5	9

In case of spring-security-saml2-service-provider all the 5 vulnerable dependencies have published a new version, where the vulnerability problems are fixed. From this perspective can be the latest library considered as secure. In the testing phase, it would be not good to stay at implementation testing, but also perform a model testing.

Discussion of Results, Recommendations or External Links to Details

Even though that within the Federated Identity Management design IDP we usually send only a fraction of identity information, like for instance belonging to some user group. In case of my bachelor's thesis minimal 3 key identity attributes are sent. The user group is represented by business category. Company registration number is expected to be used within both IDP and economic and juristic SPs and therefore it can strengthen the condition. The last of the sent attributes is the value contract validity which prevents from creating a session in case of not paid subscription. [5]

Despite of difficulties to implement, configure and maintain SAML, it is a standard that offers high level of security and can create a sense of trust between different parties by securing the sent data with signing and encryption.

From the consistency perspective the SAML messages are in format of XML which is likely to be used by older enterprise applications. In case some application would need to support a mobile device, SAML is not optimized in the way of performance for mobile devices. Even though the JSON serialization and deserialization is usually faster that the equivalent operation with XML, there are solutions for token translation where we can use both SAML and OIDC clients.

Spring Framework was chosen for its strong modularity support and its popularity within the community of Java programmers. SAML itself is not dependent on any specific platform or implementation.

To support the idea of economic firms using software based on Spring Framework, lets mention for instance an Open-Source ERP software called Metasfresh. It has a simple accounting capability and is based on Spring Framework.

While selecting the most suitable IDP, we should consider the possible Man-in-the-Middle attack and choose a solution that supports Multi Factor Authentication.

The most recommended testing is the model-oriented testing because it provides the necessary abstraction in form of state machine.

The Spring library selection was performed based known vulnerabilities of its dependencies. OWASP project contains the list of rules denoting the known vulnerabilities of web applications. These rules are updated every 2-3 years. [5] One of the tools to perform Software Composition Analysis (SCA) for checking the published vulnerabilities within the project dependencies. It is called OWASP Dependency Check. Before analysis, the tool updates itself with the most recent database from an online NIST data source.

Conclusion

Within this article I summarized the state of art concerned to SAML. The intention of this article was to bring in the SAML design topic elaborated within my bachelor's thesis. The abstract design can serve the programmer in the implementation phase and it could support him in improving fruitfulness of the future software projects. The hypothesis that security solution may help to unite multiple companies was outlined using MMDIS models. The presented solution design ought not only support collaboration, extend the user base, but also it should protect the user identity, enhance the system security, and improve the user experience while using multiple application simultaneously.

Acknowledgement

At the end I would like to thank doctors Ikuesan Richard Adeyemi and Jinyong Jo for providing me their research articles.

References

[1] Hou, W., Li, M., Liu, J., Huo., W. (2018). *Model-driven Security Testing of SAML Single Sign-On System.* Proceedings of the 2018 2nd International Conference on Advances in Energy, Environment and Chemical Science (AEECS 2018), p.335-341, ISSN 2352-5401, ISBN 978-94-6252-479-8, doi: 10.2991/aeecs-18.2018.56

[2] Jo, J., Hun, C., JongUk, K. (2019). *Development of SAML-OIDC Token Translation System for Web Single-Sign On.* The Journal of Korean Institute of Communications and Information Sciences, vol. 44, no.10, ISSN 1226-4717, doi: 10.7840/kics.2019.44.10.1928

[3] Karie, N., M., Kebande, V., R., Ikuesan R., A., Sookhak M., Venter, H., S. (2020). *Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud.* Proceedings of the Conference: 3rd International Conference on Networking, Information Systems & Security, Association for Computing Machinery New York NY United Sates, no.56, p.1-6, ISBN 978-1-4503-7634-1, doi: 10.1145/3386723.3387875

[4] Naik, N., Jenkins, P. (2017). *Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect*. Proceedings of 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK, 2017, p.163-174, ISSN 2151-1357, doi: 10.1109/RCIS.2017.7956534

[5] Rodný, P. (2021). *Návrh Single Sign-On mechanizmu pomocou štandardu SAML v moderných webových systémoch*. Bachelor thesis, r. n. FI-113156-14968, Retrieved June 2021, from https://opac.crzp.sk/?fn=detailBiblioForm&sid=14E8631BC0ED910BFDF3A033AA8B

[6] Wilson, Y., Hingnikar, A. (2019). *Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0*. Apress Media. 311 p, ISBN 978-1-4842-5095-2

Authors

Bc. Patrik Rodný
Faculty of Informatics, Pan-European University, Bratislava, Slovakia
xrodny@is.paneurouni.com
student