Journal of Natural Sciences and Mathematics of UT, Vol. 4, No. 7-8, 2019

UDC: 004.772/.773.056.523:37
Conference paper

RISKS OF ELECTRONIC IDENTITY IN EDUCATION, BY USING TWO PROTOCOLS: OPEN ID CONNECT AND SAML PROTOCOLS

Vjollca Shemshi[1], Florim Idrizi[1], Qebir Shemshi[2]

[1]* *Department of Informatics, Faculty of Natural Sciences and Mathematics, University of Tetova, RNM*

[2] *National Examination Center, RNM*

[*]*Corresponding author e-mail: vjollca.ismaili@unite.edu.mk*

Abstract

In recent years, due to the development of technology and the intense use of computers and other electronic devices, the internet has become a very important aspect of human society. The participation of social media has enabled individuals to identify themselves in wider geographic space, creating a new communion world, which has helped to connect and stay in touch with others.

Generally, an electronic identity is a tool that allows people electronically to identify themselves and thus have access to various services. Identity enables a person to be distinguished from another.

The purpose of this document is to analyze the importance of electronic identity, related issues such as reliability of information, privacy, fraud, wealth, etc., as well as the role of virtual life with real life. Two aspects of digital identities are also taken into account: encrypted identity (passwords) as well as virtual personal identities used in forums, chat blocks created by different users. The purpose of the paper is to raise awareness related to potential problems in the area of electronic identities for appropriate actions.

Keywords: electronic identity, unique logon, security of electronic systems.

1. Introduction

The ever-increasing number of applications on the Internet has led to a large increase in the number of accounts each user creates for access to internet applications. The problems that arise from maintaining several accounts as well as the tendency of security breaches through web applications, has led to the need to define some systems for electronic identification of users as well as to increase the security and privacy of the user.

Single Sign-on (SSO) is a mechanism that uses a single transaction control to allow an authorized person to access all systems or applications. This reduces the risk that administrators manage users at the central level, increases user productivity, and enables users to access more applications or services for which they are authorized. This does not mean that SSO merges account information for all services, applications, and systems, but also contains a variety of information in a single account for identifiable users [4].

The identity of natural or legal persons is determined by features such as: name, surname, address, date of birth, e-mail address, etc. Identity not only characterizes people, it also characterizes subjects, resources, and other objects' services. In the virtual world, data and features of a person are illustrated by the attributes of an electronic system. To enable access to systems, processes, or services, users must be identifiable, ie. The system should provide secure identity information. If these data are forged or unverified then reliable communication can not be realized even for a reliable infrastructure [1].

2. Review

Security and identity management in education is presented as a critical issue due to their strategic importance [2]. Implementation of access management functions should be:

- Defining a user name (identifying)
- Verifying whether the argument belongs to the user where arguments may be the password, ID card, or personal attributes (fingerprint or soundtrack)
- Ensure that the user has allowed the access level to services and data
- Ensuring that only authorized persons can obtain authorized (active) sessions, providing proper identification, retention, and authorization.
- The electronic diary is one of the educational systems used to identify and store electronic data. The electronic diary aims is to improve communication between teachers and parents, providing quick and easy access to information. Use a database that collects, processes, validates and provides data that are relevant to the educational process.

3. The purpose of the research

Today, there are three dominant standards for electronic identity implementation: OAuth, SAML, and OpenID Connect. Within the research, these technologies are at the center of our interest, in which we have analyzed their features, patterns of operation, advantages, and disadvantages, as well as the ability to expand them.

In the following, we will give an overview of the technologies being subjected to processing in our research. First of all, SAML2 and OpenID Connect protocols have been analyzed, giving an overview of their organization models. SSO members include a confusing mix of terminology. For SSO protocols, abbreviations and conditions are used for the systems involved. Below we will explain what these abbreviations and terms are and for what they are used for.

- Identity Provider (IdP) is an electronic system that is the guarantor of identity. Identity Provider (IdP) is responsible for the process of legalization and retains user information as an arbitrary value of the identity mark. When a user is authenticated, IdP creates an object that contains useful information that can be used when a service provider requests user attributes.
- Authorization server (AS) - represents the authorization server. The authorization server provides access to client arguments after successful certification. When IDP returns access tokens, then IdP also acts as an authorization server [6].
- Service Provider (SP) - is the service provider. The service provider provides security for user information [5]. When a user wants to use the security service, it requires the identification of user information.
- Client - a client is not a physical person or a firm, but a device (computer / laptop / tablet / mobile phone / etc) through which the user will have access to the service.
- User- agent - the user agent is the client's software, which is used to communicate with the protocol's servers. To search for solutions that connect Internet services to each other, a user agent is usually a web browser [1].
- Authentication is the process of identifying a person before entering the system, and then this process allows the user to enter the legalization system if he gives you access control [5]. In addition to the username and password is widely known, a check can be implemented in different ways to answer the question about secret information, One Time Password (OTP) passwords via SMS, biometric authentication tools based on digital certificates and related technologies.
- Authorization is performed after checking and setting user access restrictions. This process is usually performed on the Access Control list based on the user's role in the user group and the freedoms and restrictions set for a particular user group or the suspension of privileges for the user.
- Both OpenID Connect and SAML provide authentication and authorization, so both can be used for the same purposes, using only a few different technical tools [3]. But why we choose one or another, where the difference between these two protocols is or which gives us greater priority of use, we will present the differences between these protocols. To present the following protocols functions, we have presented the SAML and OpenID Connect protocols by graphs.

❖ **SAML Protocol**

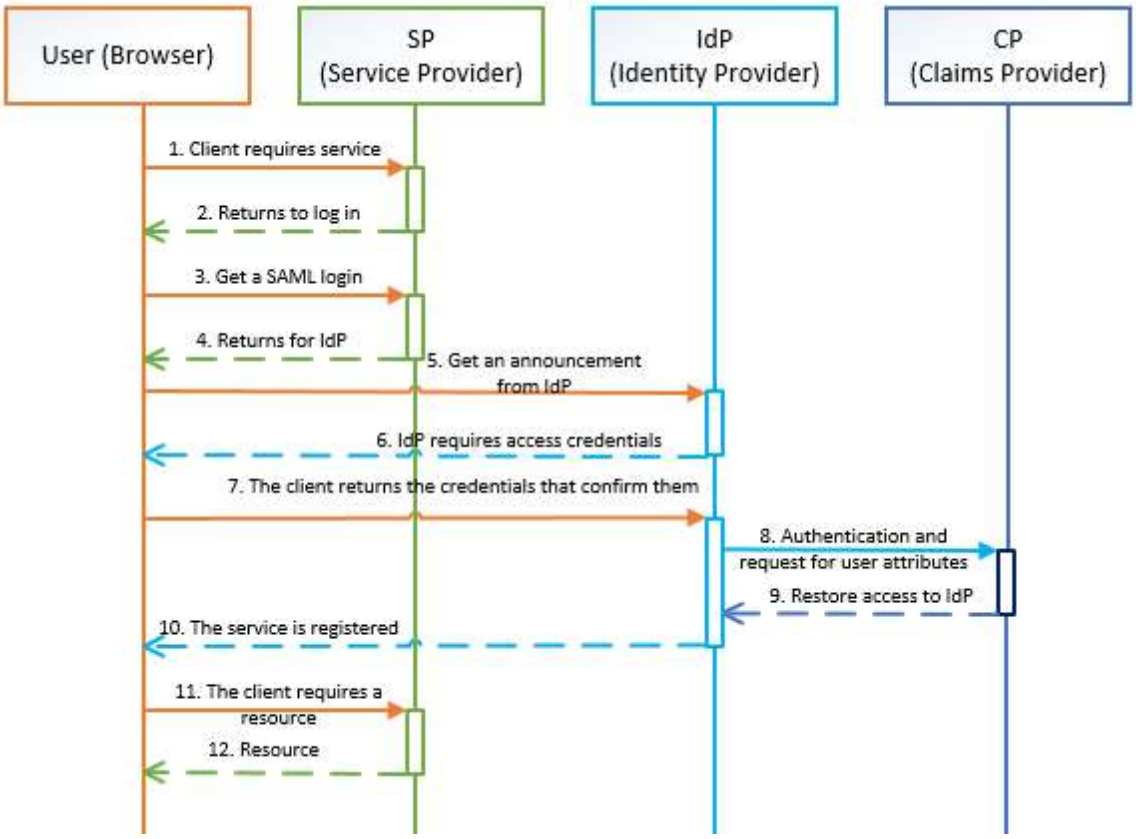

Figure 1. SAML Protocols

1. The protocol starts with a customer contacting the service.
2. The service returns the identification- request.
3. The client receives SAML identification.
4. The request is returned for identification of IdP.
5. To access the service, the client sends an IdP and AS message to request permission to access the application.
6. The IdP / AS server requires the client to provide incoming credentials.
7. The client restores the credentials of the IdP / AS server that validates them.
8. If the credentials are valid, IdP contacts with AS and requires authorization details.
9. AS returns the access point to IdP.

10. Informs the service that the user is logged in and sends an entry sign.
11. The service is registered by the client and provides access to the required source.
12. The client receives a resource.

❖ **OpenID Connect Protocols**

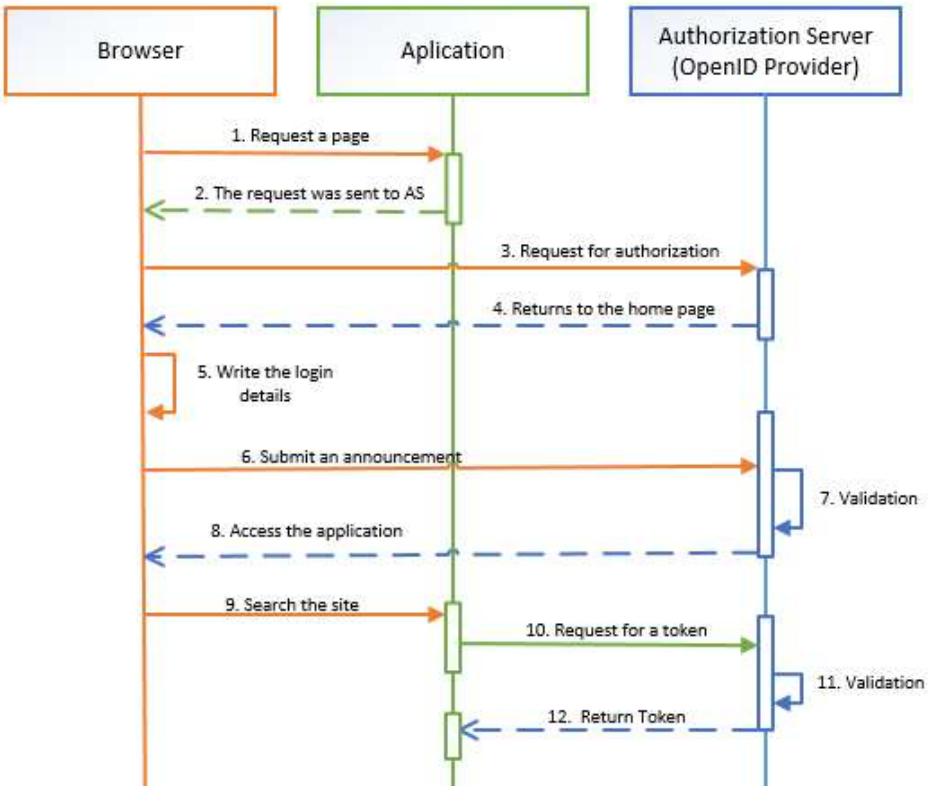

Figure 2. OpenID Connect Protocols

1. The browser communicates with the application, requesting a service.
2. The application renews the request by redirecting the authorization server to provide the dash settings. The list of input parameters is the identity list that needs to be redirected to the authorization server. Parameters that are called entry are the list of identity the application requires along with the "OpenID" value to tell the authorization server that this is an OpenID Connect request.
3. The browser sends a request to the authorization server and provides an input page.
4. This site typically includes a list of application requirements, so that the user can authorize it
5. The browser gives the login details and authorizes the publication of the information
6. Details are sent to the authorization server

7. It is verified by the user
8. Returns to the application containing the authorization code
9. The browser downloads the authorization code and downloads the application to the application
10. Then the palette request in the access point to the authorization server with the authorization code
11. The authorization server validates the code
12. And returns all the tags

a. Access sign

b. Refresh the token

c. Token ID

And the flow continues as previously defined:

OpenID Connect is a recently released protocol that uses new techniques such as JSON and REST (vs. XML and SOAP for SAML) [5]. It is designed to support web applications, local applications, and mobile applications, while SAML is designed for web-based applications only. Because XML requires a heavy content library, JSON and REST are easier to implement in the most commonly used application languages.

There is also a difference in the focus of the protocols: OpenID Connect is user-centric, while SAML 2.0 is organization-centric. Some analysts point out that the predefined set of user attributes created by OpenID Connect is more service-oriented for web service provider scenarios than for enterprise scenarios [7].

In SAML, security is implemented at the message level and uses XML-based technology for signing and encrypting messages. Also, transport level security can be implemented with TLS [8]. OpenID Connect has the opposite: transport-level security is mandatory, and message security is optional. Message security is possible through the encryption and signing of JWT objects. While SAML uses a static configuration of the metadata configuration, we can conclude that both protocols solve the same problem, but differently.

4. Conclusion

From the beginning, people have sought different ways to communicate with others. Along the centuries, communication technologies have improved and people have used communication strategies to identify themselves and distinguish themselves from others. Thus, communication has been important in determining identity. Since the Internet has become one of the major forms of communication with others, the use of social media has become one of the key forms used by people to stay in communication with friends and family.

Electronic Identification (eID) is one of the tools to ensure secure access to online services and to conduct electronic transactions more safely. Electronic identity management is the key to maintain trust in online environments that lead to economic and social development. Secure electronic identification is an important opportunity for data protection and online fraud prevention. However, there are also thefts and online frauds that represent.

References

[1]. V. Radhaa, D. Hitha Reddya - A Survey on Single Sign-On Techniques/ aInstitute for Development and Research in Banking Technology, Road #1, Castle Hills, Masab Tank, Hyderabad – 500 067 (A.P), INDIA/ 4 (2012) 134 – 139

[2]. Sh. James - Web Single Sign-On Systems/ Washington University in St. Louis/ December, 2007

[3]. Yinzhi Cao, Yan Shoshitaishvili, Kevin Borgolte, Christopher Kruegel, Giovanni Vigna, and Yan Chen - Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channe / Northwestern University

[4]. V. Radhaa, D. Hitha Reddya - A Survey on Single Sign-On Techniques/ aInstitute for Development and Research in Banking Technology, Road #1, Castle Hills, Masab Tank, Hyderabad – 500 067 (A.P), INDIA/4 (2012), 134 – 139

[5]. N. Heijmink, E. Poll - Secure Single Sign-On A comparison of protocols/ CCV & Radboud University Nijmegen/ July 27, 2015

[6]. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0/ OASIS Standard, 15 March 2005

[7]. Christian Mainka, Horst, Jörg Schwenk – On the security of modern Single Sign-OnProtocols– Second-OrderVulnerabilities in OpenIDConnect / Görtz Institute for IT-Security Ruhr University Bochum / 7 Jan 2016.