|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| VILNIAUS KOLEGIJA  UNIVERSITY OF APPLIED SCIENCES  FACULTY OF ELECTRONICS AND INFORMATICS  Image result for viko logo | | |  | | | VILNIUS COLLEGE  Image result for viko logoFACULTY OF ELECTRONICS AND INFORMATICS |
|  | | |  | | |  |
| **WEB SERVICES** | | |  | | | **INTRODUCTION TO INFORMATICS** |
| ESSAY  E-commerce analysis using web services in security aspect  6531BX028 PI18E | | |  | | | PRACTICAL ASSIGNMENT  SPOTIFY USER MANUAL  6531BX028 PI18E |
| STUDENT | SAULĖ STANKEVIČIŪTĖ | STUDENT | | DŽIUGAS PEČIULEVIČIUS |
| (SIGNATURE)  4/1/2020 | | |  | | | LECTURER |
| LECTURER | AIRINA SAVICKAITĖ | (SIGNATURE)  10/17/2018 | | VIRGILIJUS KUKLIERIUS |
| (SIGNATURE)  4/1/2020 | | |  | | | 2018 |

2020

**Table of contents**

[Introduction 3](#_Toc38505827)

[Purpose 4](#_Toc38505828)

[Goal 4](#_Toc38505829)

[Security in e-commerce with web services 5](#_Toc38505830)

[Conclusion 8](#_Toc38505831)

[Literature 9](#_Toc38505832)

# Introduction

In this day and age security is a very important aspect when we talk about contemporary technology. The idea of how much information we put out for the whole world to see does not always come across for everyday user. Starting from our names, location and ending with credit card info and other personal data, it seems as if no one is truly anonymous and if need be, people who have enough will and motive to do so, could gather enough data about the user to successfully impersonate them. To prevent that, developers must be at the front of security concepts surrounding the technology they are progressing, since the people who want to bypass the restrictions are not sleeping either. It is like a never-ending game where each player tries to outsmart the other and find the cracks and missed doors in the system to exploit. Here I will present how the e-commerce applications implement various security approaches using web services, in order to protect user data and private information from outside peering eyes.

# Purpose

Tasks include:

1. Analyze what are the core aspects of web service security.
2. Introduce levels of security in web services.
3. Analyze what approaches provide reliable security using the most popular web services.

# Goal

The main goal of this document is to provide information about how web services implement security to shield important data from being stolen or intercepted.

# Security in e-commerce with web services

There are four core aspects of web service security:

1. Authentication.
2. Authorization.
3. Confidentiality.
4. Integrity.[2]

Authentication is verifying that the user is who they claim to be. The way to identify the user is by their provided credentials, that can be of a few distinct forms. First one would be something the user has, the credentials that are issued by trusted authority (passport, smart cards). Second is something the user knows, for example, a shared secret (password).[2] Last, but not least, something the user is, such as biometric information.[2] While all these ways seem infallible, there still are ways of forging the authentication identifiers. A recommended way of approaching this part of securing the application is by using a combination of several types of credentials, for example, using an ATM card (something a user has) with a PIN (something a user knows). This is referred to as “strong” authentication. A more applicable example for the current topic would be a two-factor authentication, such as requesting a password and a confirmation through user’s phone or email.

Authorization, or access control, is granting access to specific resources based on an authenticated user’s entitlements.[2] Entitlements are defined by one or several attributes. Attributes provide information about the user in a way that the system can permit or refuse access to various areas. Some of the attacks can be executed by the people working inside the firm. Preventing damage from insider attacks is largely about limiting the amount of access a malicious insider has.[4] User attributes can limit the amount of data access the users logging from outside and inside the firm have on the e-commerce application.

Confidentiality, or privacy, is keeping information secret, that is, access a message, for example a Web service request or an email, as well as the identity of the sending and receiving parties in a confidential manner. Confidentiality and privacy can be achieved by encrypting the content of a message and obfuscating the sending and receiving parties’ identities, which is crucial to have a trusted e-commerce system.

Integrity, or non-repudiation, is making sure that a message remains unaltered during transit by having the sender digitally sign the message. A digital signature is used to validate the signature and provides non-repudiation. The timestamp in the signature prevents anyone from replaying this message after the expiration.

There are two levels of security in an application:

1. Transport-level security.
2. Application-level security.[2]

Transport-level security is a well known and widely used mechanism to secure HTTP Internet and intranet communications. It is based on Secure Socket Layer (SSL) or Transport Layer Security (TLS) that runs beneath HTTP. HTTP itself is the most used Internet communication protocol, yet it is inherently insecure because all information is sent in a clear text between unauthenticated peers over an insecure network. To secure HTTP, transport-level security can be applied.[6] It provides Authentication, Confidentiality, message integrity and secure key exchange between client and server. SSL provides a secure communication channel, however, it also has vulnerabilities. When the data is not in transit, it is left unprotected. The way this is dangerous is that the environment becomes susceptible to attacks in multi-step transactions. In other words, SSL provides point-to-point security, as opposed to end-to-end security.

Application-level security complements transport-level security. It refers to those security services that are invoked at the interface between an application and a queue manager to which it is connected. It is also known as end-to-end security or message level security.[5] Application-level security is based on XML frameworks defining confidentiality, integrity, authenticity, message structure, trust management and federation.[2]

Data confidentiality is implemented by XML Encryption, which defines how digital content is encrypted and decrypted, how the encryption key information is passed to a recipient, and how encrypted data is identified to facilitate decryption.

Data integrity and authenticity are implemented by XML Signature, which binds the sender's identity (or "signing entity") to an XML document. Signing and signature verification can be done using asymmetric or symmetric keys.[2]

Signature ensures non-repudiation of the signing entity and proves that messages have not been altered since they were signed. Message structure and message security are implemented by SOAP and its security extension, WS-Security. WS-Security defines how to attach XML Signature and XML Encryption headers to SOAP messages. In addition, WS-Security provides profiles for 5 security tokens: Username (with password digest), X.509 certificate, Kerberos ticket, Security Assertion Markup Language (SAML) assertion, and REL (rights markup) document.[2]

The SOAP envelope body includes the business payload, for example a purchase order, a financial document, or simply a call to another Web service. SAML is one of the most interesting security tokens because it supports both authentication and authorization. SAML is an open framework for sharing security information on the Internet through XML documents and this security token is particularly relevant in situations where identity propagation is essential. The protocol and bindings are taken care of by WS-Security and the transport protocol, for example HTTP.

Everything up until now was presented in favour of SOAP web service. When it comes to standardization and security, this protocol offers a better support for web service specifications. Since e-commerce applications are dealing with crucial private information like bank account numbers, it makes more sense to use SOAP, however, it all boils down to how well the API is implemented.[3] A good REST implementation can be more secure than a poorly designed SOAP implementation.

# Conclusion

In conclusion, there are four main parts of web security, that must be implemented. They include: authentication, authorization, confidentiality and integrity. With these four core parts implemented in the two layers that were discussed (transport and application layers), the development of a secure environment for e-commerce can commence. It is crucial to understand that security is a never-ending race between those who want to keep information private, and those who want to have free access to it. This means that keeping the application up to date and researching new threats and better implementations of security for the e-commerce applications is a vital step in providing a trustworthy environment for the users.

# Literature

1. Tutorialspoint.com. 2020. *Web Services - Security - Tutorialspoint*. [online] Available at: <<https://www.tutorialspoint.com/webservices/web_services_security.htm>> [Accessed 1 April 2020].
2. Docs.oracle.com. 2020. *Understanding Web Services Security Concepts*. [online] Available at: <[https://docs.oracle.com/cd/E17904\_01/web.1111/b32511/intro\_security.htm#WSSEC1508](https://docs.oracle.com/cd/E17904_01/web.1111/b32511/intro_security.htm%23WSSEC1508)> [Accessed 1 April 2020].
3. Apica. 2020. *Understanding Security And Dependability For SOAP And REST*. [online] Available at: <<https://www.apicasystems.com/blog/understanding-security-dependability-soap-rest/>> [Accessed 1 April 2020].
4. Liquidweb.com. 2020. [online] Available at: <<https://www.liquidweb.com/blog/five-common-web-security-problems/>> [Accessed 1 April 2020].
5. Ibm.com. 2020. *IBM Knowledge Center Error*. [online] Available at: <<https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q010610_.htm>> [Accessed 1 April 2020].
6. Ibm.com. 2020. *IBM Knowledge Center*. [online] Available at: <<https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/twbs_secwsaatl.html>> [Accessed 1 April 2020].