Nov 8th, 12:15 PM - 12:30 PM

Authentication in SaaS by implementing double security measures

Muhamet Gërvalla
University for Business and Technology, mgervalla@gmail.com

Shkëlqim Berisha
University for Business and Technology, shkelqim.berisha@ubt-uni.net

Authentication in SaaS by implementing double security measures

Muhamet Gërvalla[1], Shkëlqim Berisha[2]
[12]University for Business and Technology,
mgervalla@gmail.com[1], shkelqim.berisha@ubt-uni.net[2]

Abstrakt. Growing trends of services offered in the field of Cloud Computing are increasing on daily basis. These services are divided into three models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Despite this, much interest is shown to the usage of Software as a Service (SaaS) model. This model offers the usage of software's that are hosted in Cloud that can be accessed by using web browsers or through "thin client". Security and privacy are two most important problems that can occur in this model. Authentication through password is one of the best methods known as authentication through a parameter. However this is not a safe technique because the password can be easily broken through man-in-the-middle method and other attacks. Being aware of this problem we come to the need of using another technique for authentication known as authentication through two parameters that offers better solution to this problem. This technique allows users to ensure two parameters during the phase of authentication, parameters that are combined together to create a high security. This authentication technique should be used to secure all services and software's that are offered in Cloud.

Keywords: authentication, security, Software-as-a-Service, cloud computing.

1 Introduction

Growing trends of services offered in the field of Cloud Computing are increasing on daily basis [4]. These services are divided into three models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Despite this, much interest is shown to the usage of Software as a Service (SaaS) model. This model offers the usage of software's that are hosted in Cloud that can be accessed by using web browsers or through "thin client" [5].
Security and privacy are two of the most important problems that may be encountered in this model. Software as a Service is a Cloud Computing model, this model is offered by different provider who provide services in this model. Nowadays security concerns are increasing in all areas of information technology. There are some issues when dealing with security concerns that are directly related to the password for authentication. Most systems to verify the identity of users use static passwords. This is an unreliable method since an attacker can easily find these passwords using various methods known as snooping, sniffing, man-in-the-middle etc.
There are many different strategies proposed that serve for authentication [1]. Some of which are more difficult to apply and some are not suitable for users of these services. Authentication through two parameters is one of the proposed techniques. There are different methods of how this technique can be applied.
This paper will provide a technique which provides a secure and verified solutions for authentication problem. This method allows users during authentication to be used an algorithm which randomly generates a 5 digit number which will be sent to the personal phone number of the user where the user must then use that code to connect to services offered in SaaS in second step of authentication. The cost of using this method is very low when compared to the importance of problem for sensitive systems.

2 Definition of the problem

In most cases, the security of data is guaranteed by the provider of services for users of Software as a Service. The service provider must ensure that different users cannot access the data of other users. This is a very crucial point to ensure the integrity of user's data [3]. Authentication is the process of verifying

whether we are dealing with the requested identity. There are four different methods known worldwide that are used for authentication, they are: via password, tokens, ID cards or in a biometric manner. There have been a lot of research to find different alternatives that serve to provide us security [2]. Authentication via password is one of the best methods known as authentication through a parameter. This technique is not very secure because an attacker can easily break passwords who use various techniques to attack. This was very important reason to offer a solution to the problem of authentication in SaaS.

3 System design and implementation

In this paper will be proposed a method for authentication, it would be a good method which can replace common authentication methods that are currently used in SaaS. This method works by using two different parameters that will be used for authentication in two steps. The first parameter is the password of the user and the second parameter is a 5 digit number which is generated by the system which serves to authenticate in second step. To implement this we have developed an application that consists of three parts which are interconnected in the process of authentication: Client Side, Server Side and Database.

3.1 Client Side

In this part like in any form that serves to authenticate to the system we will have first step where data will be filled like the username and password of the user. If these parameters are registered in the database of the system and parameters are valid then the system will pass on to the second step of the system in which must be completed the second parameter.The second parameter is a 5 digit code that will be generated automatically by the system when the username and password of the user are valid. Once the code is generated the code will be firstly added to the database by the system, then the code will be sent to the personal phone number of the user, where the user must fill in the second part which serves for authentication.

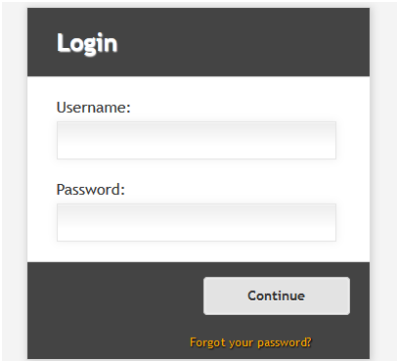

Fig 1. Authentication form in first step

If the user has successfully completed the first part of the user and password but has given the incorrect code for 3 times which is sent by SMS to the phone then this code will be not valid for use, furthermore if 3 minutes pass after the system has sent this SMS to the user personal number and does not enter it in the second part of the authentication process then this code will be regarded as invalid. In this case, the user must restart the authentication process from the beginning.

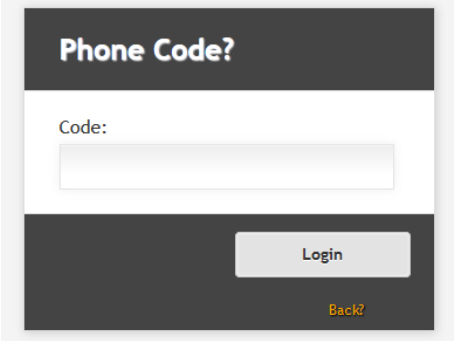

Fig 2. Authentication form in the second step

If the user fulfills properly the first step of authentication and the second step where the code is then the user is authenticated successfully.

The code which is sent by SMS to the user cannot be used 2 times to authenticate.

3.2 Server Side

Server should be implemented in such a way as to be able to generate a 5 digit number, to be able to send these codes to users of system via SMS, make the validation of the parameters received from the client, check number of attempts to login with a code that was generated once, check the expiry time on which a code is valid for authentication after generation, and to assess whether it can proceed with authentication if the parameters are properly given.

Fig 3. The authentication process

3.3 Database

Database on the server serves to save user information like name, user, password, phone number for each user. Also, for every attempt to authenticate must create a record of authentication details like time of attempt, user identity, code and password.

4 Conclusion

Using SaaS service has many advantages, but also some weaknesses, especially in the field of data security and privacy. One of these problems is the method of authentication to these services. Until now,

various techniques have been proposed for authentication. One of these techniques is authentication through one parameter, this is an unreliable technique since there are various methods which the passwords can be obtained from an attacker like man-in-the-middle etc.
The work done in this paper is intended for use in SaaS. Most of the services offered in this technology use the authentication method which in most cases is done only from the service provider. To provide safe services in this technology in this paper is offered a solution by implementing dual authentication parameters. The solution which is offered is an interaction between the software of the server, the user of the services and SMS offered by a phone operator. A technique which provides a high-level security while it resists various attacks by malicious attackers.

5 Future Work

Because of the danger that exists from various attacks which can occur in communication between service providers of SaaS and SMS service operators, in the future we need to find a solution which will be used to encrypt data which are sent from the software system of the server to the SMS service operator. Communication between these two points should be made in this way: when a user fills correctly username and password, the software in the system should create a secure connection between the server and the SMS service operator. In this case, an algorithm should be developed which will make the data encryption that will be transferred between these two points. The application that needs to be developed should be implemented in the SaaS service provider and also in the SMS service operator.

References

1. A. Josang and G. Sanderund, “Security in Mobile Communications: Challenges and Oppurtunities," in Proc. Of the Australasian information security workshop conference on ACSW frontiers, 43-48, 2003
2. Sagar Acharya, Apoorva Polawar, P.Y.Pawar, “Two Factor Authentication Using Smartphone Generated One Time Password”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 2, 2013, 85-90
3. Choudhary V.(2007). Software as a service: implications for investment in software development. In: International conference on system sciences, 2007, p. 209
4. Vidya Prakash, Recent Trends in Cloud Computing: A Survey, International Journal of Advances in Computer Science and Technology, 2013, http://warse.org/pdfs/2013/ijacst04252013.pdf.
5. Automation Services, Basware Corporation, Chandigarh, INDIA, SaaS (Software as a Service) Based Business Model: Cost Analysis, International Journal of Management and Commerce Innovations (IJMCI), 2014.