Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):27-31

Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

DEVELOPMENT OF AUTHENTICATION PROTOCOLS WHEN ACCESSING CLOUD SERVICES

O. Oksiiuk, V. Chaikovska

Taras Shevchenko National University of Kyiv

ABSTRACT.

Cloud services are a rapidly developing industry, but rapid development is accompanied by many problems. One of such problems is unsafe authentication, which leads to the theft of confidential information. The problem of theft the access to the account is discussed all over the world. In this article, the authentication protocols that are being used, modified and developed by scientists and developers were reviewed. The presence of a large information base indicates that this problem is urgent and requires solutions.

Key words: authentication, protocols, secure connection, information security, cloud services.

Cloud services are a rapidly developing industry, but rapid development is accompanied by many problems. One of such problems is unsafe authentication, which leads to the theft of confidential information.

The object of the study is the process of secure authentication in cloud technologies. The subject of research is new authentication algorithms.

The purpose of the work is research the current direction in the development of the scope of authentication protocols in the cloud.

Cloud authentication has the following common features:

- For user convenience, one-time remote authentication mechanisms are used when accessing various cloud services;
- To interact with cloud services with the authentication service, you need to use widespread protocols and access control standards;
- use international experience and best practices;
- It must be provided with an authentication information security service.

Following these features, a large number of algorithms are created for hacking this process.

The problem of theft the access to the account is discussed all over the world. Many scientists propose to solve in many ways [1-3, 5]. Also in the previous year a book dedicated to this problem was published [4].

On such services as github and gitlab, everybody can also find working algorithms of authentication protocols.

Developers of programming languages also develop and refine libraries for writing authentication algorithms.

All this indicates that the threat of cyberattacks on the authentication process is relevant all over the world.

The main tasks of information security for "cloud" calculations are:

• secure remote registration;

• Safe account management;

• secure deletion of authentication and trust in cloud services;

• trust management with the interaction of cloud services;

• the sharing of user access and access control in anchor to the user authentication method, its role and requirements to the level of trust in the cloud;

• provision is subject to control according to the time (in length) of the access with the guarantee of a break of the session after the expiration of the specified time of access.

Classification of attacks on "cloud" services:

1. Traditional software attacks.
2. Functional elements of the attack on the clouds.
3. Attacks on the client.
4. Attacks on the hypervisor.
5. Attack on the management system.

Managing access of users to information resources is traditionally one of the most complex tasks in the field of information technology. When switching to cloud computing and services, this task becomes even more complex and relevant.

Intruders and information security engineers expect the greatest risks from users. They are most vulnerable during the transition to cloud computing, that is, during authorization.

The Cloud Security Alliance (CSA) is the most effective way to protect clouds of cloud computing. After analyzing the information published by the company, the following solutions were proposed.

1. Data storage. Encryption

Encryption is one of the most effective ways to protect data. The provider providing access to the data must encrypt the customer information stored in the data center, as well as, if not necessary, irrevocably deleted.

2. Data protection during transmission

Encrypted data during transmission should be available only after authentication. Data can not be read or modified, even if accessed through unreliable nodes. Such technologies are quite known, algorithms and reliable protocols AES, TLS, IPsec have long been used by providers.

3. Authentication

Authentication - password protection. For higher reliability, tokens such as tokens and certificates are often used. For the transparent interaction of the provider with the system of indetting for authorization, it is also recommended to use LDAP and SAML.

4. Isolation of users

Using an individual virtual machine and a virtual network. Virtual networks must be deployed using technologies such as VPN, VLAN and VPLS. Often, ISPs isolate user data from each other by changing code data in a single software environment. This approach has the risks associated with the danger of finding a hole in a non-standard code that allows access to data. In the event of a possible mistake in the code, the user may receive data from another. Lately, such incidents have often taken place.

At the moment, modified versions of old protocols are used around the world, which makes it possible to improve the algorithms already developed and make them more crypto-resistant.

Some of them:

1. NTLM is a network authentication protocol developed by Microsoft for Windows NT. The protocol operates on a request-response basis, but the server does not send a password, but sends a hash created using the server's returned key and user account data. Next, the server checks the transmitted hash locally and accordingly allows either no access to the resource.

2. Kerberos offers a mechanism for mutual identification of the client and the server before establishing a connection between them. It is based on the use of markers, tickets. When using this protocol, the client first transfers the login and password to the authentication server. In response, the server returns an authentication token. This token can then be used when accessing resources on the network, without the need to transfer account information (user name / password) over the network and re-authenticate. Also, Kerberos authentication is used to solve the 'double-hop' problem. The essence of the problem lies in the need to access some network resource or server from the code using the credentials of the user that caused the code.

3. The technique of two- and more-factor authentication has long been used in various areas of information security, and at the moment, many popular web services include the possibility of multifactor authentication. For example, after Google and Amazon, Twitter, Dropbox and LinkedIn were also involved in the game. At the same time, most services use the OTP mechanism as a second factor. In addition, that this method is not very convenient (each time you have to wait for SMS, or run a special application, or generate a password on an OTP token and then enter it with pens), OTP has a number of vulnerabilities - the possibility of phishing and, in addition, the need for storage on OTP Generator secret server in clear. The bitter experience of well-known and not so companies has finally taught us how to use persistent hashing of passwords, after which the need to store OTP secret in an open form looks strange, to put it mildly. To ensure the secure storage of authentication data on the server, it is necessary to use asymmetric cryptographic algorithms. I'll discuss these issues further in the text of the article, but for now I'm offering the reader the main difficulties that arise in the development of a multifactor authentication system.

4. Six variants of mathematical models of authentication during users work with mobile applications in cloud area are represented: with application server, with applications forms, on certification, with one-time parole, on accesses keys, and with tokens. Three factors symbol description for authentication classification for chois their models is given. The three level seven factor approach to identifications classification for model identification is given. The intelligence approach for choice of identification and authentication system (IAS) on the base of expert system (ES) knowledge base roles is proposed. The model of decision support system in ES may be based as on expert approach such as on automatic regime of server.

Nowadays the idea of avoiding passwords and traditional methods of authentication on web resources is rising more and more, and this has taken care of such giants of the IT industry as Google, Paypal and other members of the FIDO alliance. As part of research carried out by Google employees, methods of improving authentication methods were proposed, as well as a draft of the TLS extension standard, which allows to get rid of the use of cookies.

The transition to such technologies should be as simple as possible, so it is necessary to establish the following requirements:

- The technology should not require the installation of additional software that goes beyond the browser and its extensions
- A single device should be sufficient to store data to a number of websites on which a user is registered

- The registration and authentication protocols should be open and should not rely on third party services. It is very important to note here that other parties should not enter into the relationship of the user and the site, since the user trusts the site (this is facilitated by SSL)

The browser plus plug-in at the same time must provide the site with two APIs: for registration of new users and for authentication. When a new account is created, the service calls the registration API, resulting in the generation of a new key pair on the device, the public key of which is stored on the server. Later, this key will be used to confirm the identity of the user as follows: using the authentication API, the server transmits a request to the user, who signs it and returns it.

The TLS ChannelID extension provides a mechanism for extending the TLS protocol, which allows you to get rid of the transfer of authentication tokens (English, bearer token), such as HTTP cookies or OAuth tokens.

A TLS extension with which you can create a long-term channel between the client and the server that will be stored between various HTTP requests and TLS sessions, if these connections originate from the same client device.

The essence of this method is that after initial authentication instead of cookie on the client device, a key pair is generated, the public key of which is stored on the server. Later, when the TLS-connection (TLS handshake) is established, the client proves to the server that it owns the private key, and the public key is the Channel ID. This method is better for using cookies for several reasons:

A private key never leaves the client device, so an attacker can not intercept a secret from the channel

All cryptographic operations can be performed on a separate device, which protects the private key from stealing directly from the client side.

To authenticate in real time with the use of standard equipment, the parameters of the keyboard handwriting and subject's faces that are registered during operation on the computer are suitable. However, these technologies in practice so far are characterized by a high number of authentication errors of subjects. This work is aimed at improving the reliability of the procedure for continuous authentication in real time in the space of these characteristics.

Also, there is an idea of a secure authentication algorithm for web resources without using HTTPS, which allows you to save the password protected from an attacker. The key idea of this algorithm is not to send the user's password to the server in the clear. Instead of the password, it is suggested to send the encrypted hash from the password, which. The essence of this approach is that if an attacker intercepts an encrypted password hash and if he can decrypt it, he will receive only a hash with salt from which it is already impossible to obtain the original password.

Keystone—OpenStack's Identity service—provides secure controlled access to a cloud’s resources. In OpenStack environments, Keystone performs many vital functions, such as authenticating users and determining what resources users are authorized to access.

In this article, the authentication protocols that are being used, modified and developed by scientists and developers were reviewed. The presence of a large information base indicates that this problem is urgent and requires solutions.

First, it is obvious that traditional password authentication should be supplemented in other ways. Secondly, with the advent of a large number of devices, users need to develop a reliable way to authenticate these devices. Thirdly, it is possible to single out the trend of the "shift" of the levels of account security: if earlier two-factor authentication was used mainly in RB services, now it has moved to the sphere of public accounts. From this, we can also conclude that the RBS services themselves now require more rigorous authentication methods than OTP.

REFERENCES:

1. Filimoshin V. Yu. Davletkireyeva l.z.: Secure authentication without using https. - International Journal of Open Information Technologies (2017) 7, 17-23.

2. Khazhieva A. S.: Principles of information protection in the cloud. - Achievements of science and education (2017) 6(19), 14-16.

3. Lozhnikov P., Sulavko A., Buraya E., Pisarenko V.: Authentication of Computer Users in Real-Time by Generating Bit Sequences Based on Keyboard Handwriting and Face Features. - questions of cyber security (2017) 3(21), 24-34.

4. Steve Martinelli, Henry Nash, Brad Topol: Identity, Authentication, and Access Management in OpenStack: Implementing and Deploying Keystone. - O'Reilly Media, 2016 – 130.

5. Vishniakou U.A., Ghondagh Saz M.M.: Authentification models in cloud computing for mobile applications with intellectual support of choice. – Doklady BGUIR. - Electron resource: https://www.bsuir.by/m/12_104571_1_112204.pdf#page=82, 2017.