UDC 004.56

O. Oksiiuk, V. Chaikovska

UNSAFE AUTHENTICATION AS ONE OF THE CLOUD SERVICE PROBLEM

The problem of saving personal data is very serious. Since most people switch to storing their data in the cloud, various types of attacks on the authentication process become a great problem. It is the easiest way to unauthorized users take over other people's files. 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 actions. First, traditional password authentication should be more protected and not stored by all meanings. Secondly, with the various number of devices, users need to come up with the reliable way to authenticate these devices. And thirdly, it is possible to use two-factor authentication instead of single sign on, as it can be used not only in companies but a simple person.

***Keywords*:** authentication, protocols, confidential information, secure connection, information security, cloud services, cybersecurity.

1 Formulation Of The Problem

Cloud services is a rapidly developing industry, and many problems accompany it. One of such issues is unsafe authentication, which leads to the theft of confidential information. The object of the study is the process of secure authentication in the cloud technologies.

The subject of research is the fundamental problem of 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 common features: • For user convenience, one-time remote authentication mechanisms are used when accessing various cloud services;

• To interact with cloud services and the authentication service, you need to use widespread protocols and access control standards;

• Using international experience and best practices;

• It must be provided with an authentication information security service.

There are a lot of hacking methods based on these features.

While technology is developing, the need for improving the cybersecurity is increasing as well.

The continuous cloud technology development and the development of high-speed networks have become as necessary as air and water. Cloud usage formats include not the only Infrastructure as a Service (IaaS), which accelerates the shift from ownership to use of infrastructure resources but also Platform as a Service (PaaS), which provides a platform for developing and executing applications.

Most access systems require the users to authenticate using a username and password combination. This method of authentication relies on the password's secretiveness and in some cases, even the username's secretiveness. If this secretiveness is not breached, the assertion is that this pair uniquely identifies a user. The number of problems are associated with maintaining password secrecy like passwords having birthdays, anniversaries, common words or terms related to a particular user which are universally considered vulnerable since it is easy for an attacker to guess them or find this information on social pages.

Some systems require users to remember complicated passwords or/and usernames - the more complicated user recalled that it is better. Of course, also involved usually means "difficult to retain" which is a usability liability. It is challenging for the users because other people (e.g., system administrator) choose complicated passwords, but they also must pick them repeatedly, since different systems have different rules for username as well as password generation. The user can have many username-password pairs. The primary purpose is ensuring that the compromise of a single password doesn't compromise them all. In practice, though many users are overwhelmed by remembering so many unique and complicated username-password pairs that they don't fully comply with guidelines provided by the system – typically, using the same or very similar password for all accounts. However, even if they follow the best-recommended practices, hackers still easily steal passwords, whether transferred inadvertently or not: users sometimes write passwords down on a piece of paper, store them in text files, and accidentally expose them by entering them in the username field and so on.

The problem of access theft is discussed all over the world. Many scientists propose to solve it in many ways. Moreover, it was published the book about this problem.

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.

And these aspects indicate that the threat of cyberattacks on the authentication process is relevant all over the world.

2 Features Of Cloud Technology Security

The cloud storage service provider maintains a cloud storage that for providing the necessary infrastructure to create, store and update outsourced databases, and makes this data available to the clients. Customer has to be an organisation, a group of sensors, or any other logical abstraction of a cloud user. The clients are given read-only access to the database, and authorized clients are allowed to make (limited or unlimited) queries in the database. The system also comprises of entities called data sources that originate the data to be stored on the cloud, and are responsible for creating and maintaining the cloud database. Both clients and the data sources can range from powerful computers to capability-restricted (i.e., storage-, computation-, communication- and power supply restricted) mobile devices and other connected things.

More precisely, the top four threats identified are: data leakage, data loss, account hijacking and insecure APIs. The externalized aspect of outsourcing can make it harder to maintain data integrity and privacy and organizations should include mechanisms to mitigate security risks introduced by virtualization. Especially when they deal with sensitive data, such as health records, the protection of stored information comes as a top priority. Therefore, data security can be seen as the foundation upon which the entire transition to a cloud architecture should be based. Multiple risks must be addressed in order for an organization to guarantee the safety of users' records. One of the most important aspects is security of sensitive information. To this end, the deployment must ensure that all sensitive data is stored in encrypted form. Complementary to this, proper key management must ensure that encryption keys are not revealed to malicious users.

The main tasks of information security for "cloud" services 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 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 indexing 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.

3 Methods Of Protection And The Authentication Protocols

Now, 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 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.

In recent years, enterprises want to get convenient and flexible information infrastructure through the cloud computing. However, information security issue of cloud computing has been one of the threshold for enterprise to adopt cloud computing. In order to solve the cloud security issues, enterprises began to deploy private cloud. SSL virtual private network (VPN) gateway is a solution for enterprise to securely access private cloud services. There are two main types of SSL VPN gateway, i.e. SSL Portal VPN and SSL Tunnel VPN.

IT administrators may integrate existing account of active directory or lightweight directory access protocol (LDAP) to SSL VPN gateway. Therefore, IT administrators can easily configure SSL VPN gateway to control the different groups of users which can use what kind of resources and applications. Besides, SSL VPN gateway provides mobile one-time password (MOTP) to enhance security authentication.

As we are passing our data through internet, we need to check that our data is secure not only at storage but also when it is transmitted through different channels. To achieve this, network security parameters should be considered. Firewall and gateways should be setup appropriately to avoid hackers entering and stealing valid data. We also need to make use of secure communicating layers and protocols to avoid data loss by intruders. We can make use of secure socket layer for communicating. Other options include HTTP over SSL which is called HTTPS. Other alternative to HTTPS is secure HTTP (SHTTP). Depending on what kind of security mechanism we need to deploy for our application, we should decide on the communication protocols considering its pros and cons.

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, a high number of authentication errors of subjects so far characterizes these technologies in practice. 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.

References:

1. Cloud Standards Customer Council. Security for Cloud Computing Ten Steps to Ensure Success Version 2.0. – 2015. – 35p.
2. Filimoshin V. Yu. Davletkireyeva l.z.: Secure authentication without using https. - International Journal of Open Information Technologies (2017) 7, 17-23.
3. Hickey K. Dark cloud: Study finds security risks in virtualization / Kathleen Hickey // Technology, Tools and Tactics for Public Sector IT. - 2010 - № 3 — p. 3-5
4. Khazhieva A. S.: Principles of information protection in the cloud. - Achievements of science and education (2017) 6(19), 14-16.
5. 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.
6. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing / National Institute of Standards and Technology / Rebecca M. Blank. – Gaithersburg: NIST, 2011. – 286 p.
7. Vishniakou U.A., Ghondagh Saz M.M.: Authentification models in cloud computing for mobile applications with intellectual support of choice. – Doklady BGUIR. - Electronic resource: https://www.bsuir.by/m/12_104571_1_112204.pdf#page=82, 2017.
8. Winkler J.R. Securing the Cloud. 1st Edition / Vic (J.R.) Winkler. - US : Syngress, 2011. - 314p.
9. Prakash Chandra Srivastava, Anupam Agrawal, Kamta Nath Mishra, P. K. Ojha, R. Garg,"Fingerprints, Iris and DNA Features based Multimodal Systems: A Review", IJITCS, vol.5, no.2, pp.88-111, 2013.DOI: 10.5815/ijitcs.2013.02.10. http://www.mecs-press.org/ijitcs/ijitcs-v5-n2/v5n2-10.html
10. Hamdy M. Mousa,"DNA-Genetic Encryption Technique", International Journal of Computer Network and Information Security (IJCNIS), Vol.8, No.7, pp.1-9, 2016.DOI: 10.5815/ijcnis.2016.07.01. http://www.mecs-press.org/ijcnis/ijcnis- v8-n7/IJCNIS-V8-N7-1.pdf
11. Stewart I.: Life's other secret: the new mathematics of the living world. Penguin, New York, USA (1999).
12. Seberry J., Wysocki B.J., Wysocki T.A.: On some applications of Hadamard matrices. Metrica, 62, pp. 221-239 (2005).
13. Harmuth, H. F.: Sequency theory. Academic Press, N.-Y., USA (1977).
14. Morita Y., Sakurai Y.: Holography by Walsh Waves. In: Proceedings of the Symposium (4th) Held at the Catholic University of America, Washington, D. C. on 16-18 April, pp. 122-126 (1973).
15. Karpovsky M.G., Stankovic R.S., Astola J.T.: Spectral Logic and its Applications for the Design of Digital Devices. John Wiley & Sons Inc., New Jersey, USA (2008).
16. Belousov L.: Morphomechanics of Development. Springer International Publishing AG, Switzerland, (2015).
17. Pribram K.: Languages of the Brain. Englewwod Cliffs, New Jersey, USA (1971).
18. Jenuwein Th., Allis C.D.: Translating the histone code. Science, v. 293, pp.1074-1080 (2001).
19. All-or-none law. https://en.wikipedia.org/wiki/All-or-none_law (this page was last modified on 26 March 2017).
20. Penrose, R.: Shadows of the Mind. Oxford University Press, Oxford, England (1996).
21. Yaglom I.M.: The Boolean Structure and its Models. Sovetskoye Radio, Moscow, USSR, 1980 (in Russian).
22. Schrödinger E.: What is life? University Press, Cambridge, England (1955).
23. Varfolomeev S.D.: Chemical enzymology. Akademia, Moscow, Russia (2005).
24. Hamilton A. Invention of the year. The retail DNA test. Time, Oct. 29 (2008).
25. Petoukhov S.V.: The genetic code, algebra of projection operators and problems of inherited biological ensembles. – http://arxiv.org/abs/1307.7882, 8th version of the article from 3 May 2017, pp. 1-93 (2017).
26. Davis P.J.: Arithmetics. – In: "Mathematics in the modern world", Scientific American, N. Y., USA, p. 29-45 (1964).
27. Pavlov D. G.: Leading article. Hypercomplex numbers in geometry and in physics, 1(1), p. 4-7 (2004) (in Russian).
28. Russel B.: A History of Western Philosophy. - Book One, Part I, Chapter III. Simon & Schuster/Touchstone N.Y., USA (1967).
29. Heisenberg W.: Physics and Philosophy: The Revolution in Modern Science. Penguin Classics N.Y., USA (2000).

Надійшла: 15.05.2018 Рецензент: к.т.н. Довбешко С.В.