МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2020
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2020
Proceedings of the Forty-ninth Spring Conference
of the Union of Bulgarian Mathematicians
2020

VERIFICATION OF USER IDENTITY AND DATA SECURITY IN THE CONTEXT OF LMS AND LCMS*

Oleg Iliev, Radoslav Yoshinov, Georgi Tsochev

Modern education offers a variety of methods and tools for online learning. Nowadays, learning management systems are a tool that facilitates modern learning. That is why the security of these systems in terms of user authentication and verification is an important element. This raises the issue of providing data security at an extremely high level and also obliges the system to provide a way of verifying users identity. The article presents opportunities to meet these requirements through a combination of cryptographic algorithms, the use of flexible software architecture, and a user identification model.

Introduction. At present, information systems are an essential component in our everyday life. Central to the entire information and communication infrastructure are the computer networks, which are crucial for delivering many services for people and businesses: web applications, e-learning, e-commerce and others information society service [1]. The advent of the Internet is a major concern and alongside with it is the network and information security. Common security issues occur when creating a new system from basic browser authentication to physical access to servers. The authors of e-learning systems place more emphasis on functionality than the security when building such systems and this is why this document focuses on common security issues when developing new information systems.

The Learning Management Systems (LMS) and the Learning Content Management Systems (LCMS) must be constantly adapted to the evolution of technology, they must provide the most accurate information to the learners, tailored to their personal preferences and presented in the most attractive way possible. Moreover, these systems are no longer available just locally within one university, but accessible from anywhere in the world. This will either turn them into huge monolithic applications whose support will require enormous efforts and where the security remains a weak link, or seek a more appropriate and modern way to create a flexible, scalable, reliable and secure software architecture. E-learning course contains sensitive information, user data, and other content that must be kept from unauthorized access [3]. The paper presents exactly the kind

*2020 **Mathematics Subject Classification:** 68N19, 94A62, 94A60.

Key words: learning management systems, security, authentication, authorization, cryptographic algorithms.

This research is supported through the ICT in SES program of the Ministry of Education and Science of the Republic of Bulgaria.

of architecture that focuses on outsourcing responsibility for user authentication and authorization to a single service using Service Oriented Architecture (SOA), securing user data, and verifying user identity, as a must in a system where participants cannot be identified directly.

Extracting the responsibility for user authentication and authorization. Sharing multiple responsibilities from one system leads to its overload, lack of flexibility and scalability. The main business logic that is expected to be addressed in LMS and LCMS is related to the context of learning. Adding logic that deals with user authentication and authorization would unnecessarily complicate the system. Moreover, the protection of this module becomes much more difficult as it goes through to ensure maximum protection of the whole system. In other words, instead of concentrating on a small part of the system, the computer scientists have to deal with the whole system. This kind of a software architecture design has a huge drawback – releasing a new version of the learning-related business logic requires a release of the authentication and authorization system and vice versa [4]. The solution to this problem is to extract the logic to an autonomous service that will run and will be maintained independently of the entire system. In addition to dealing with the aforementioned problems, the use of an independent system that communicates with the core system enables the use of this system from more than one application. A good way to achieve independence between different parts of the system is to introduce SOA, as shown in the graph below (Fig. 1).

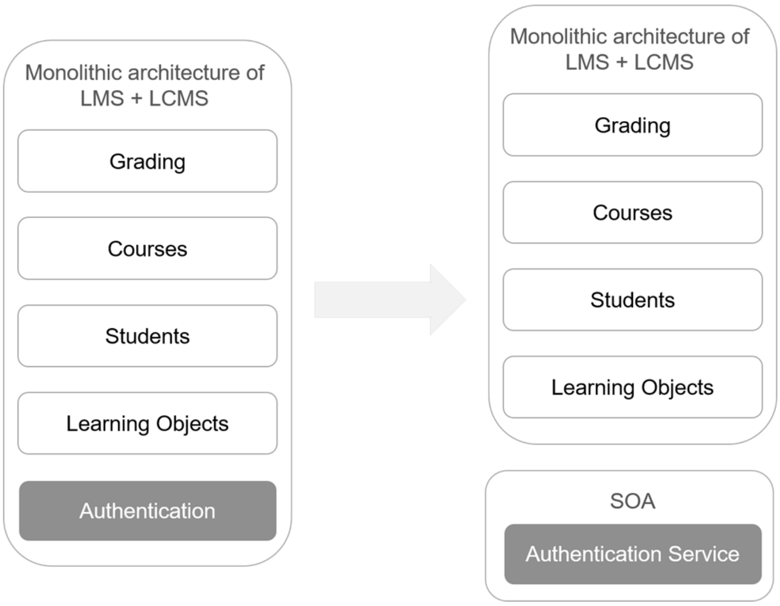

Fig. 1. Extracting the authentication logic into SOA

The SOA architecture provides many advantages of the system, such as flexibility, scalability and reliability [2]. It also makes it easy to configure a continuous the delivery (CD) and continuous the integration (CI) process.

Creating an authentication and authorization system for users from scratch involves a lot of work and the risks of not keeping the latest software trends for maximum security. Instead, an open source based solution could be used in the face of Identity Server. This is a web based service that integrates seamlessly with any web based software system, enables management of user roles and privileges from a centralized location, and provides a single sign-on (SSO) entry point [5].

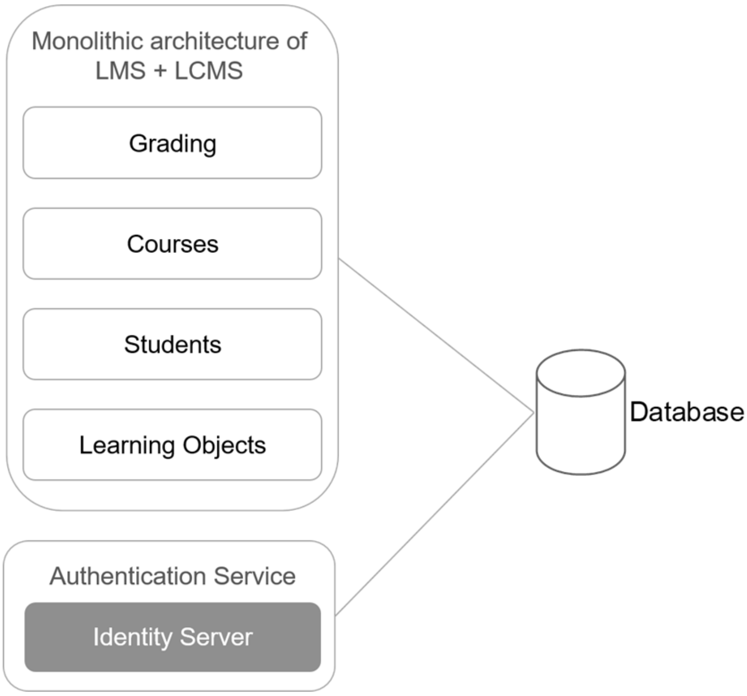

Fig. 2. Integrating Identity Server into LCMS + LMS architecture

Thanks to the Identity Server, one could easily provide the support of an external source of user authentication, such as a Facebook or a Google user account. This is achieved by the common user authentication standard OAuth2 (Fig. 2).

User authentication is handled by a central point and then a token is generated in the form of a Globally Unique Identifier (GUID) that represents the user to any individual applications part of the architecture. In other words, unlike Basic Authentication (where by principle the username and password are sent, encrypted or formatted, to the server, along with any requester) here only a GUID is sent, which means nothing to a malicious person who can “sniff” the traffic generated by the app. This GUID is verified by the Identity Server and applications gain access to a variety of user claims through which they can authenticate the user to individual parts of the system.

Ensuring the security of user data. Extracting the logic related to user authentication is a very important condition for maximum security in LMS and LCMS, but not sufficient is the user data protection is concerned. To compromise the security of this system would mean to get access to the users' passwords stored in the database. The easiest way to protect them or other data that would allow the unauthorized use of the user account (account cracking), such as the answer of a secret question, is by hashing this secure data. Many systems do this by encrypting the data instead of hashing it, thus breaking the encryption key could break the security of all data encrypted with it. At the same time using the key is necessary by the system's architecture to ensure a two-way "unlocking" and "locking" the data. The systems that use hashing often use the MD5 algorithm, which is well known and has already been cracked by the so-called "brute force" attack and the use of a dictionary of potential password values in the hashed and non-hashed versions.

Ensuring maximum data security requires a combination of cryptography and hashing algorithms. One of the most secure algorithms at the moment is the Password-Based Key Derivation Function 2 (PBKDF2), which uses a key to hash and further encrypt data with SHA-512 (Secure Hash Algorithm). It almost completely eliminates the possibility of using brute force attack to crack the protected data. It requires the use of a key, so the computer specialists must again be careful, since if the key is breached by "malicious person" this would lead to complete compromise of the data protected by it. For this reason, it is important to select the most secure key. The use of so-called cryptographic "salt" that provides randomly generated data used as a key can be a solution to this problem. The developed data protection mechanism presented in this article assumes that generation of *salt* is based on a GUID which is then coded to the Base64 and finally stored in the database, as shown in the graph below.

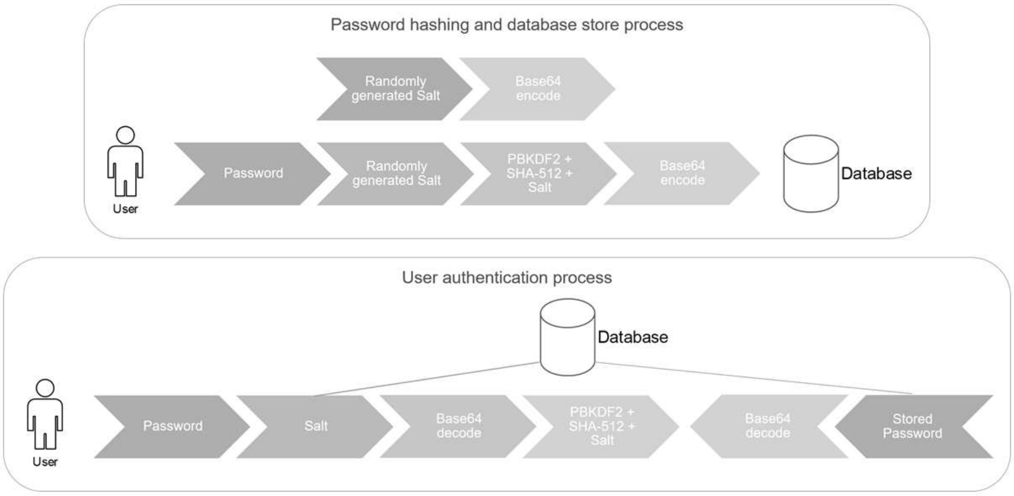

Fig. 3. Process of user registration and further authentication

The authentication process goes through the creation of a user account with a password encrypted with PBKDF2 in combination with SHA-512 and using a different *salt* per each user. After the account is created, the user's provided password is being hashed during the authenticated process, as it was done when the account was created, and this result is compared with the password saved in the database, without the need to "unlock" the password stored into the database. In other words, even the system administrator of the LMS and LCMS will not be able to understand the user's password.

Verification of user's identity. The modern learning and content management systems offer a virtual environment in which the user (teacher or student) consumes learning materials, generates content, assesses his/her knowledge, and also has the opportunity to obtain a certificate attesting to his/her completed training course. In other words, these types of systems aim to completely replace the conventional method of offline training, whereby all participants in the learning process meet in person and the verification of their personalities becomes easy and direct (the learner is introduced to

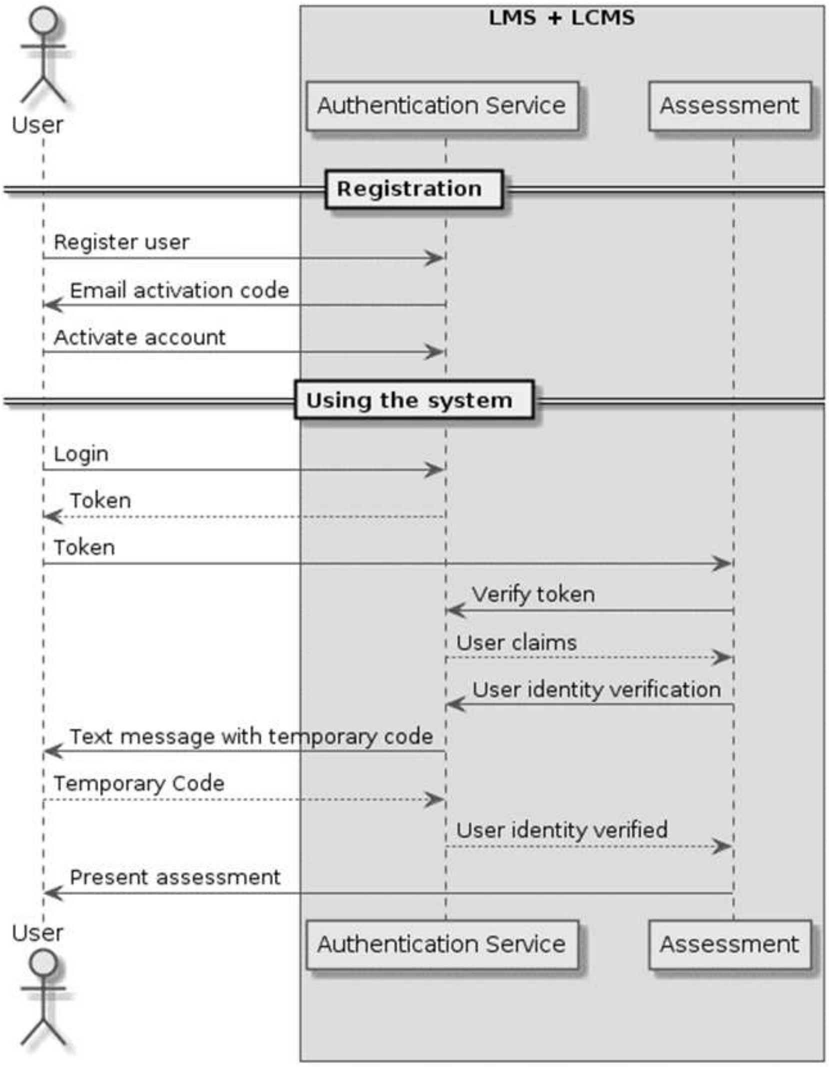

Fig. 4. User authentication and identity verification

the teacher and both know each other), with one in which the connection between all participants in the process is virtual (authentication and verification of individual participants in the process is necessary for them to present themselves to the system and from there – to the other participants). For this reason, it is absolutely necessary to ensure that the consumer identity can be verified.

Even with the provision of a highly reliable service for a user authentication and authorization, the human factor runs the risk of compromising the process. Users can be expected to be careless when storing or using their passwords. This raises the question: "How can we be sure that the user posing as a teacher is indeed the one and not someone using the teacher's account maliciously?". The same question is applicable also for the students, who have the opportunity to receive a certificate at the end of a course.

According to the General Data Protection Regulation (GDPR) [6], binding to more than one user authentication method ensures that consumer identity is fully identified. In other words, the combination of a username and a phone number is a sufficient way of verifying a user's identity [7]. Following this idea, various services are now available over the Internet to enable third party verification of the user's identity instead of using well-known electronic signatures. For example, the DocUSign system provides the ability of having a fully legitimate and legally enforceable contracts signed remotely by the users. With LMS and LCMS it is possible to simultaneously associate email, username and phone number.

During the registration process into the LMS or LCMS the user chooses a username that makes it unique to the system, then he/she is required to enter an email to use to communicate with him/her and confirm his/her registration by going to the address cited in an automatically generated email to activate the account. This provides the system with the ability to link the personal email address of the user with a unique identifier for the system in the face of the username. Further, if a code is sent to the user's phone number as part of a text message during any user's attempt to interact with the system, such as when starting an exam or when generating a learning content, one can be assured that the system provides verification of the user's identity. It is not possible for a malicious person to impersonate the user since even "stealing" the password is not enough to interact with the system.

Conclusion. The migration of any individual part of a system to SOA has many advantages, such as providing scalability, reliability and flexibility to the individual modules that are expected to have higher load than the others. At the same time, the system business logic can be separated in order to completely differentiate responsibilities. The user authentication service is a suitable module to be exported when we talk about LMS and LCMS. In this way, the system can retain the learning-related logic at its core, and authenticate the users with another system that can even be used by several systems at the same time.

Following this idea, it should also consider the actual protection of user data that is stored in the database and which could potentially compromise the users' accounts. Furthermore, in the case of real security breach, the system must provide a way to verify user's identity, as a prerequisite for a system where individuals cannot be identified directly. The paper offers a software architecture, a direct example of its integration into an LMS or LCMS, and a modern way of verifying user's identity, which is a promising solution to such problems.

The use of advanced training also brings many security concerns, such as social engineering and hacking. They will always participate and the only thing that can be done is to try to the tighten security not only through software and hardware solutions, but also by introducing an additional measure. Future work includes deeper investigation of the verification of the user, more specifically – by creating user profile and monitoring its activity based on different technologies, such as microservice architecture or agent based technology.

REFERENCES

[1] R. Graziani, A. Johnson. Routing protocols and concepts. Indianapolis, IN 46240 USA, Cisco Press, 2008.

[2] M. Conde-González, F. García-Peñalvo, M. Guerrero, M. Forment. Adapting LMS architecture to the SOA: an Architectural Approach., 322–327, 10.1109/ICIW.2009.54, 2009.

[3] K. El-Khatib, L. Korba, Y. Xu, G. Yee. Privacy and Security in E-Learning. *International Journal of Distance Education Technologies* **1**, *4* (2003), 1–19, doi: 10.4018/jdet.2003100101.

[4] A. Baier, T. Bernoulli, T. Braun, C. Graf, U. Ultes-Nitsche. Case Study of the Usage of an Authentication and Authorization Infrastructure (AAI) in an E-Learning Project. Proceedings of the ISSA 2006 from Insight to Foresight Conference, 5–7 July 2006, Sandton, South Africa, 10 pp.

[5] R. Vasiu, A. Ternauciuc, M. Onita, B. Dragulescu. Single Sign-On Solutions for Moodle. Conference proceedings of "eLearning and Software for Education", issue:01, 2009, 217-224.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679, Accessed 2019-06-27.

[7] D. Amo et al. GDPR security and confidentiality compliance in LMS' a problem analysis and engineering proposal. A: International Conference on Technological Ecosystems for Enhancing Multiculturality. TEEM'19: Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality: León, Spain, October 16–18, 2019. New York: Association for Computing Machinery (ACM), 2019, 253–259.

Oleg Iliev
e-mail: ilievo@cc.bas.bg
Institute of Mathematics and Informatics
and
Laboratory of Telematics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Block 8
1113, Sofia, Bulgaria

Radoslav Yoshinov
e-mail: yoshinov@cc.bas.bg
Georgi Tsochev
e-mail: gtsochev@cc.bas.bg
Laboratory of Telematics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Block 8
1113, Sofia, Bulgaria

ВЕРИФИКАЦИЯ НА ИДЕНТИЧНОСТТА НА ПОТРЕБИТЕЛЯ И СИГУРНОСТТА НА ДАННИТЕ В КОНТЕКСТА НА LMS И LCMS

Олег Илиев, Радослав Йошинов, Георги Цочев

Модерното образование предлага достатъчно разнообразни методи и средства за онлайн обучение. В днешно време системите за управление на обучението са едно от основните средства в помощ на съвременното образование. Именно и затова сигурността на тези системи, от гледна точка на потвърждение за автентичност и удостоверяване на идентичността на потребителя, е важен елемент. Това повдига въпроса за осигуряването на сигурност на данните на изключително високо ниво и също така задължава системата да осигури начин за проверка на идентичността на потребителите. Статията представя възможности за изпълнение на тези изисквания чрез комбинация от криптографски алгоритми, използване на гъвкава софтуерна архитектура и модел за идентификация на потребителя.