MANAS Journal of Engineering

Volume 6 (Issue 1) (2018) Pages 75-83

Comparison of the Security Mechanisms of Document Management Systems

Mahabatkan Tashtanova*, Rita Ismailova

[1] Kyrgyz Turkish Manas University, Department of Computer Engineering, Bishkek, Kyrgyz Republic
mahabat.tashtanova@manas.edu.kg; rita.ismailova@manas.edu.kg

Received: 12-01-2018; Accepted: 20-03-2018

Abstract: As the demand of the current level of ICT development, management also turns to the use of computer technologies. As a result, there are many document management systems are emerging. The use of computer technologies not only decreases the use of documents in paper form and saves time, but also preventы from document lost during the management process. In this study, several document management systems were selected and their security mechanisms were compared. Security criteria such as identification by username, authentication by checking passwords, authorization mechanisms, access control determination and accountability were compared.

Keywords: *Document management system, security, confidentiality, integrity, digital signature*

Электрондук документ айландыруу тутумдарынын коопсуздук механизмдерин салыштырмалуу талдоо

Аннотация: Мезгилдин талабына ылайык учурдагы мамлекеттик башкаруу же башкаруу тутумдары да техникалык өзгөрүүгө умтулушууда. Мисалы, электрондук башкаруу менен документтерди электрондук түрдө айлантуу. Документтерди кагаз түрүндө эмес электрондук түрдө айлантуу менен: убакыт үнөмдөөгө, документ айлануу процесиндеги колдон колго өтүү менен документтин жоголуп кеткен учурларынан коргоого жана аз болсо да керексиз чыгашалардан кутулууга ээ болобуз. Бул изилдөөдө бир канча докумен айлантуу тутумдары тандалып, алардын коопсуздук механизмдери салыштырылган. Салыштыруу, иденттештирүү, колдонуучу ысымы (username), аутенттештирүү (тастыктоо), сыр сөз (password), авторизациялоо, документтерди көрүү (жазуу, алмаштыруу) уруксатын берүү (access determination) жана көзөмөлдөө мүмкүнчүлүгү (accountability) боюнча жүргүзүлдү

Ачкыч сөздөр: *Электрондук документ айланттуу, коопсуздук, жашыруундук, маалыматтын толуктугуна келтирилген коркунуч, санарип кол кою*

* Corresponding Author.

1. INTRODUCTION

We are living in the era of engineering and technology development and with the use of the technology, we are able to solve a waste variety of problems. In accordance with the demands of the time, the information and communication technologies and control systems are being used not only on the level of organization management but even in the management processes at the governmental level. The main task of the modern-day technology experts is to provide the correct and a high-speed information transmission. Since the waste majority of the management processes are also making use of internet technologies, changing the way we manage documents is also a natural step and it comes out as the turnover of documents in electronic form.

By convert document flow from a paper form to electronic form has several advantages. First of all, it saves time, and secondly, by eliminating the manual delivery where a document pass through many people and storages, we prevent its lost during transmission and delivery. In addition, the cost of a document management decreases due to decrease of the use of paper. However, along with all these advantages, the transition to the electronic document flow can be time-consuming and a hard task to perform at the beginning of the transition process. This is due to digitization of databases with large amounts of data, which may take time to transfer documents in electronic form.

In the implementation process of any system, regardless of its simplicity or complex structure, there are certain rules that must be followed. These rules are important since any device, connected to the internet, becomes a part of a system of systems. Organization of a document flow with the opportunities, provided with internet technologies are really enormous. On the other hand, when a device is connected to some network, potentially, any document stored in this device is accessible by any object in a network. Therefore, development of secure platforms for the document flow becomes a big challenge for the office professionals and developers.

Ensuring compliance with the security requirement while implementing a document management system of an organization is one of the new fields of data protection. The main issues with a document management systems are that in companies, not only the stored data but also, phone numbers the employees, addresses, etc. are also considered as a sensitive information. Moreover, this information is continuously being processed and transmitted. This, the security mechanism in a document management system should deal not only with confidentiality of an information while storage, but also with the integrity of information while processing and transmitting, and availability of information for all authorized users of the document management system.

2. LITERATURE REVIEW

a. Electronic document management systems

According to Glinskih [1], an electronic document management system is a collection of mechanisms and documents of an agency or company, which enables the whole cycle of document creation, transmission and processing until some decision is made based on this document. The system should satisfy some requirements, such as auditing, which means that every action in a system should be recorded and stored in a database. By action in an electronic document management system we mean not a physical action, but the access rights and security clearance level of each user and security classification of each document. Thus, the secure implementation of an electronic document management system starts with the administrative rules set by an agency and the system should be designed with the clear vision of these principles. Mostly, this type of electronic document management system is utilized by government agencies, commercial organizations or industrial companies, that is, every agency with internal document flow. Thus, depending on the configuration of systems, they can manage the small amount of document in small organizations up to big datasets in large companies and governmental agencies. They provide not only the effective and efficient document management, but also allow a collective work on the set of documents. One of the first computer-based document management systems is dated back in 1988 by Kawell et al. [27]. Another system was patented in the USA and was used to manage semi-electronic and paper-based documents [26]. The document flow in a system was defined by automatically importing, indexing, categorizing and storing documents. In addition, the system allowed a search, retrieval, manipulation and archiving electronic documents. With the development of information science, there was a development in the implementation of an electronic document management systems as well. For example, a system DocMan by Bäcker and Busbach was used not only to perform above-mentioned operations. It was also designed to provide some level of awareness to its users such as sending notifications if other users see or work with the same documents [28].

Since an electronic document management systems are powerful tools that impartially decrease the time for document processing and its cost, the use of such systems is increasing every day. With the help of electronic document management systems, companies can conduct agreements, make financial calculations, correspondence, and deliver documents and other data [12]. Timely implementation of document management systems can provide high-capacity for a company.

b. Security mechanisms in an electronic document management systems

Prohorov and Kuzinyak (2005), claim that one of the main advantaged of electronic document management systems is that they allow access restriction to an information [2]. That is, depending on the security level of an information, the system protects the information from an unauthorized access by users with lower security clearance by using access control models. This advantage of electronic document management systems was investigated by many researchers from different aspects. For example, Dosmuhamedov, (2009) showed the graphical model of an electronic document management system. In this model, the system was considered from two perspectives – possible vulnerabilities from the inner attackers and from outer attackers [3]. The analysis of security mechanism was conducted. According to the results, the threats were divided into three main categories, which are:

- Threats to confidentiality,
- Threats to integrity,
- Threats to the availability of information.

Also, he discussed the possible sources of these threats and possible consequences of attacks. Azhmuhamedov (2010) proposed to use marking signs for the hidden documents in electronic document management systems [4]. In 2011, Daurzev proposed a model to evaluate the compliance with security requirements in a system and the efficiency of information protection [5]. In his work, Eliseev, (2012) tried to analyze the possible destructive influence on electronic document management systems leading to the loss of the legal significance of the electronic document when uploaded to an electronic document management system [8]. Another study of the legitimacy of an electronic document was conducted by Vishnevskiyi et al. (2014), where a systematic analysis of information properties in computer-based document management systems was done. As a result, it allowed classifying a new complex threat for information systems, where the legislation is a priority - the threat of "loss of legal force by a document in electronic form". The main indicator reflecting the realization of the threat of loss of legal force in an electronic document is the negative result when verification by a digital signature. Taking into account the technical features of information processing in electronic document management systems, the validity of digital signature means that if a document, signed with some digital signature algorithm, was modified, then the validation process fails since a new signature will not match with an original one [10]. The analysis of threats was conducted, and according to the obtained results, they were divided into six groups depending on the type of threat. In addition to the three categories, defined in [3], in this work, 3 more categories were considered, thus, these six threats are:

1) The confidentiality of the electronic document - the availability of an electronic document only to authorized users (or processes);
2) The integrity of the electronic document - the permanence of certain elements of the electronic document at all stages of its life cycle, regardless of the ways and means of processing an electronic document;
3) Availability of the electronic document - the ability to access certain elements electronic document and presenting them in the required form for a certain time for authorized users;
4) The legitimacy of an electronic document - the appropriateness of the technology used during the life cycle of an electronic document;
5) Reliability of the electronic document - full and accurate reflection in the electronic document of the confirmed operations, activities or facts;
6) The authenticity of an electronic document - compliance with the declared nature of the electronic document, as well as the time, place and author, claimed in the electronic document

Before computer-based electronic management systems were developed, security mechanisms for protecting an information were mainly concentrated on the security of documents [6], however, now, the vector of attacks has changed. In this work, authors considered the optimal way of ensuring efficient security by optimization of all possible security mechanisms available to a company. As it can be seen, there are many security mechanisms. Suhovey et al. (2012) claim that security systems in enterprises consist of various specialized systems, such as cryptographic and biometric systems, that circulate information within some closed cycle. These systems are to achieve certain goals, however, they do not interact with each other [7]. The authors propose to combine the authentication of users and the electronic document management system into a single security system, based on the application of bio-cryptographic methods.

Other authors, such as Bychkov et al. (2013) used comparative method while considering an electronic document management systems. They compared five systems in five dimensions, namely, 1) an authentication of users, including levels of authentication; 2) access control models; 3) availability of mechanisms for a digital signature; 4) encryption of data in selected systems, and 5) system logs and accountability of systems [9]. Although in the selected systems all the mentioned features were present, authors suggest using additional mechanisms to protect electronic document management systems from real-time attacks as well. There are many studies where the usage of cryptographic mechanisms, including digital signature use in an electronic document management systems was analyzed [11], [29].

Other authors, such as Drovnikova et al. (2016) considered technical aspects on security in systems, such as network security mechanisms, use of firewalls, as well as the use of appropriate access control models [14], [15], [16].

3. MATERIALS AND METHOD

a. Revised electronic document management systems

As it was mention before, there are many electronic document management systems available. Some of these systems are commercial systems, while others are open source. In the scope of this study, several document management systems were selected. As a main criterion in the selection was an availability of open source codes of systems. However, development of a document management system is very expensive and complex task. Therefore, some systems, included in an analysis, are commercial ones. We selected nine software, namely:

- NaumenDMS[1] [17]
- LetoDMS[2] [18]
- KordilEDMS[3] [19]
- Opendocman[4] [20]
- Alfresco[5] [21]
- Deskaway[6] [22]
- Knowledge Tree[7] [23]
- OpenKM[8] [24]
- SGB Net [9]

Mostly, these applications are web-based. Thus, the analysis was conducted via the internet. As a limitation of this work we would like to mention that since some applications were commercial, only a demo-versions were analyzed.

[1] http://www. naumen. ru/go/products/for_small_business/naudoc
[2] http://www. letodms. com/
[3] http://www. kordil. net/
[4] http://www. opendocman. com/
[5] http://www.alfresco.com/products/dm
[6] http://www. deskaway. com/about/index. php
[7] http://www. knowledgetree. com/
[8] http://www. openkm. com/
[9] http://sgb.manas.edu.kg/

b. Method

In this study, we have utilized a comparative method. The basic features, which were included in the comparison process were the followings:

- Availability of user identification mechanisms
  - Username (username)
- Availability of user authentication mechanisms (confirmation)
  - Password (password)
- User authorization
  - access determination
- Control (Accountability)
  - User control (track whatever user does)

The comparison was done manually. First, we have installed systems with an open source code. For the web-based system, requests for a demo version were sent. In addition, a documentation of systems was carefully analyzed.

4. RESULTS AND DISCUSSION

In this section, to avoid ethical and legal issues we do not name document management systems. The result of the analysis showed that all nine system, included into the analysis, support user identification and have an admin panel. Mostly, these systems have some predefined document types (that is, seven out of nine examined systems) and option for document achieving (again, seven out of nine examined systems). Also, among selected nine systems, two were web-based applications. Also, as an additional features, there were

- Notification via e-mail (in two systems);
- File upload option (in two systems);
- Search engine;
- Audit;
- File versions management;
- Mobile version is available;
- Search engine.

Some other features were observed in a few systems only; the digital signature option was available in NaumenDMS system only. Also, many systems do not have multilingual support.

The main objective of the waste majority of attacks is gaining access to the information source. In an electronic document management systems, to ensure the confidentiality of documents (files), we need to ensure the security of the whole system. In addition, not only the data within the system but also the system itself must be protected. Therefore, security measures should be carried out: a complex organization and management of the physical hardware equipment, software, peripherals, and verification measures, as well as support and audit of a system [13].

In the scope of this study, we have tested nine systems for the availability of basic security mechanisms. One of the main week points in software-based systems is that many of them work over HTTP rather that https protocol. Another notable point is that in some of the tested systems, vulnerabilities listed in reports by OWASP (Open Web Applications Security Project - Open Web Tirkemererinin Security Project) were found. Also, as other researchers also noted, no cryptographic tools, such as digital signature algorithms, are implemented to verify data [25]. Thus, a document management systems are used as information storage systems only.

In addition, for any document within an electronic document management system, a legal significance (or validity) of the electronic document must be preserved when uploaded to an electronic document management system [12]. This is considered to be one of the basic requirements in computer-based systems, and in order for this requirement to be met, the electronic digital signature needs to be developed for the legislation. In addition, to electronically sign documents within such systems, PKI (Public Key Infrastructure) must be developed.

If a company is established within the jurisdiction of two or more countries, the problem with the document management and PKI standards of the two countries can arise as well. Thus, while developing or adoption of an electronic document management system, many aspects should be taken into account.

5. CONCLUSION

In the life-cycle of electronic documents, its confidentiality, integrity, and availability are the main issues. However, it is impossible to overcome all security threats by setting up a single event. Security is a continuous process, not a product.

As a result, for the document management systems to be secure, we need to develop the infrastructure. In addition, with the development of information and communication technologies, the need for good specialists in this area is also rising. According to one of the most basic principles of information security states that the system is as secure as its weakest chain. Moreover, many researchers agree that users are the most vulnerable part of the system. Therefore, there is need to not only focus on the development of technologies, but also give a priority to increasing the advancement of technology and computer literacy of system users. In the Kyrgyz Republic, there are many technical high schools, thus, we believe that the development of the information technology sector is a matter of time only.

In this regard, the regulation rules should also be carefully re-considered by government agencies so that legislation on the information security would be efficient. The state bodies and institutions should address the problem that led to improving the quality of activities, the need to develop a legal and regulatory framework and agreements since the problem of digital signature use in document management systems is directly related to this issue.

REFERENCES

[1]. Glinskih A., Mirovoi rynok system elektronnogo dokumentooborota. Jet Info Informacionnyi byulleten, 8 (111), (2002).

[2]. Prohorov A., Kutsinyak D., Dokumentooborot i ego programnoye obespecheniye, Computer Press, 1, (2005),172-176.

[3]. Dosmuhammedov B.R., Analiz ugroz informatsii system elektronnogo dokumentooborota, Vestnik Astrahanskogo Gosudarstvennogo Tehnicheskogo Universiteta, Seriya Upravleniye, vychıslıtelnaya tehnika i informatika, 2, (2009), 140–143.

[4]. Ajmuhamedov İ.M., Markirovka pechatnyh kopi konfidensiyalnyh elektronnyh dokumentov, Vestnik Astrahanskogo Gosudarstvennogo Tehnicheskogo Universiteta, Seriya Upravleniye, vychıslıtelnaya tehnika i informatika, 1, (2010), 7-9.

[5]. Daurtsev A.V., Sposoby kompleksnoy otsenki effektifnocti programmnyh sistem zashity v avtomatizirovannyh sistemah elektronnogo dokumentooborota, Vestnik Voronejskogo Gosudarstvennogo Tehnicheskogo Universiteta, 3, (2011), 7.

[6]. Buldakova T.İ., Glazunov B.V., Lyapina N.S., Otsenka effektivnosti zashity sistem elektronnogo dokumentooborota, Doklady Tomskogo Gosudarstvennogo Universiteta, Sistem upravleniya i radioelektroniki, 1-2, (2012), 25.

[7]. Suhovey A.A., Gonçarov S.M., Elementy biokriptografii na osnove otpechatkov paltsev v sisteme bezopasnosti predpriyatiya. Vestnik Morskogo Gosudarstvennogo Universiteta, 51, (2012), 151-159.

[8]. Eliseev N.İ., Model ugroz bezopasnosti pri ee obrabotke v sisteme zashishennogo elektronnogo dokumentooborota, İzestiya Yujnogo Federalnogo Universiteta, Tehnicheskiye nauki., 12, (2012) , 137.

[9]. Bychkov S.S., Popov A.M., Obespecheniye informatsionnoy bezopasnosti ve sistemah elektronnogo dokumentooborota, Reshetnevskiye chteniya, 17, (2013), 139-140.

[10]. Vishnevskiy A.K., Eliseev N.İ., Finko O. A., Analiz ugroz bezopasnosti informatsii v sistemah elektronnogo dokumentooborota, IV Vserosiyskaya nauchno-tehnicheskaya konferensiya, Oktober 10-13, Russia, Sank Peterbugr, (2013), 64-70.

[11]. Rezenkov D.N., Tuturjans N.B., Kriptografiya element zashity elektronnogo dokumentooborota, Kultura i obshestvo: İstoriya i sovremennye materialy III Vserosiyskaya nauchno-prakticheskoy konferensiya, Russia, Stavropol, (2014), 91-95.

[12]. Magomedov M.S., Murtuzaliyeva N.M., Sistemy elektronnogo dokumentooborota-problemy zashity. VII Mejdunarodnaya studencheskaya elektronnaya nauchnaya konferensiya, Russia, Studencheskiy nauchnıy forum, (2015).

[13]. Markova S.B., Bezopasnost elektronnogo dokumentooborota, Prikladnye issledovaniye i tehnologii. Sbornik trudov II mejdunarodnoy konferentsii 2015, Russia, Moskow, (2015), 185-189.

[14]. Drovnikova İ.G., Rogozin E. A., Zastrojnov İ.İ., Konseptualnaya model upravleniya zashitoy informatsionnogo resursa sistemy elektronnogo dokumentooborota, Vestnik Voronejskogo Gosudarstvennogo Tehnicheskogo Universiteta, 2, (2016), 147-154.

[15]. Serova N.A., Aktualnye problemy zashity elektronnogo dokumentooborota, Gosudarstvennoye i munitsipalnoye upravleniye v XXI veke: teoriya, metodologiya, praktika., Novosibirsk, 26, (2016), 189-193.

[16]. Rogozin E.A., Obuhova L.A., Analiz osobennostey funksionirovaniya programmnyh sistem zashity informatsiiv v sistemah elektronnogo dokumentooborota. Obshestvennaya bezopasnost, zakonnost i pravoporyadok v III tysyachaletii, 1-2, (2016), 347-350.

[17]. NaumenDMS. Source: http://www.naumen.ru/go/products/for_small_business/naudoc [access date: 10.09.2017]

[18]. LetoDMS. Source: http://www. letodms. com/ [access date: 10.09.2017]

[19]. KordilEDMS. Source: http://www.kordil. net/ [access date: 10.09.2017]

[20]. Opendocman Document management system. Source: http://www.opendocman. com/ [access date: 10.09.2017]

[21]. Alfresco Document management system. Source: www.alfresco.com/products/dm [access date: 10.09.2017]

[22]. Deskaway Document management system. Source: http://www.deskaway.com/about/ index. php [access date: 10.09.2017]

[23]. Knowledge Tree Document management system. Source: http://www.knowledgetree. com/ [access date: 10.09.2017]

[24]. OpenKM Document management system. Source: http://www. openkm. com/ [access date: 10.09.2017]

[25]. Küçükşen D., Integrated Public Financial Administration Systems Pre-Analysis Project: Example of Needs Assessment Questionnaire. ICEBEG 2017: International Conference on eBusiness and eGovernment. Book of Abstracts (2017).

[26]. Chen Y.J.J., Ferguson D.R., Hong A.N., Suleman D., Whittemore G.L. *U.S. Patent No. 6,009,442*. Washington, DC: U.S. Patent and Trademark Office. (1999).

[27]. Kawell Jr,L., Beckhardt S., Halvorsen T., Ozzie R., Greif, I. Replicated document management in a group communication system. In Proceedings of the 1988 ACM conference on Computer-supported cooperative work, ACM, (1988), 395.

[28]. Backer A., Busbach U. DocMan: A document management system for cooperation support. In System Sciences, 1996., Proceedings of the Twenty-Ninth Hawaii International Conference on, IEEE, 3, (1996), 82-91.

[29]. Astahova T.S., Chadaeva E.P., Elektronnaya sifrovaya podpis kak faktor sohraneniya celostnosti i audentichesnosti dokumenta, Izvestiya Tomskogo politehnicheskogo universiteta, 320(6), (2012).