Security of Collaborative Banking Systems

ION IVAN, CRISTIAN CIUREA
Department of Informatics and Economic Cybernetics
Bucharest University of Economic Studies
Piata Romana 6, Bucharest
ROMANIA
E-mails: ionivan@ase.ro, cristian.ciurea@ie.ase.ro

Abstract: This paper presents theoretical elements regarding collaborative systems. There are described their properties and implementations of collaborative systems in economy are analyzed. Security requests regarding collaborative banking systems are identified and solutions to increase collaborative systems security level are proposed. The security is analyzed starting from the authentication process and there are presented security elements for collaborative systems after and outside the authentication.

Key-Words: collaborative systems, security, informatics applications, implementation, banking.

1 Collaborative Systems

Collaborative systems are the new generation of intelligent and auto-adaptive systems, encountered in many fields of the economy. In [1] and [2], collaborative systems are defined as interactive systems. Collaborative work leads to success if all team members demonstrate motivation and responsibility. Collaborative and social nature of teamwork is appreciated in designing interactive systems.

In order to consider a system to be collaborative, this system must be in accordance with followings concepts: communication, coordination and cooperation [3].

There are many criteria to classify collaborative systems existing in the economy. By manner of components organization, collaborative systems have linear, tree or network structure. The field of application allows classifying collaborative systems as follows [4]:

- collaborative banking systems;
- collaborative micro-payment systems;
- collaborative educational systems;
- collaborative planning systems;
- collaborative tagging systems;
- collaborative writing systems;
- collaborative medical systems.

Figure 1 presents the collaborative systems classification by field of application and highlights the importance of collaborative banking systems.

Collaborative Banking Systems
Collaborative Educational Systems
Collaborative Tagging Systems
Collaborative Planning Systems
Collaborative Writing Systems
Collaborative Medical Systems

Fig. 1. Collaborative systems classification

The banking system is the most significant collaborative system, because it has a large number of components and a large variety of links between them [5]. The banking information system must be collaborative, because it requires the communication, coordination and cooperation of different informatics applications, in order to achieve a common goal.

2 Implementations of Collaborative Systems in the Economy

There are many implementations of collaborative systems in the economy, in different areas of interest and in both environments: real and virtual.

In the real environment, there are many types of collaborative systems, the must important being the collaborative banking systems, collaborative educational systems and collaborative systems in production.

In the virtual environment, the collaborative systems implemented are represented by the virtual campus, the virtual bank, the virtual enterprise for software development and the virtual enterprise for production processes.

Figure 2 shows the place in space-time coordinates of collaborative systems implemented in real and virtual environments [6].

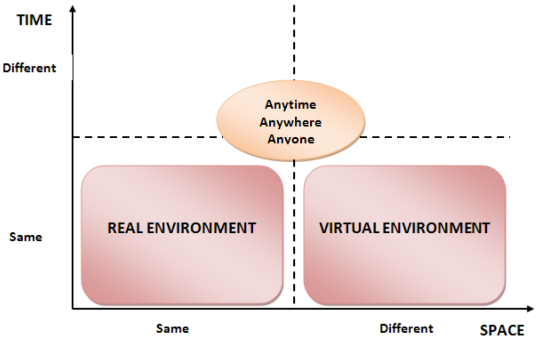


Fig. 2. Real and virtual environments

There are many aspects that must be taken into consideration when analyzing the differences between collaborative systems implemented in real environments and the ones implemented in virtual environments.

If the case the collaborative system implemented in real and virtual environments is represented by a university, then the comparison between classical education and online education reveal that the assimilation of knowledge is made more efficient in the case of online education, due to the process of collaborative learning within the teams.

3 Security Requests

The security of collaborative systems is an important issue that must be analyzed in order to identify security requests, to discover possible vulnerabilities or threats and to avoid loss of information.

Security of collaborative systems requires the existence of the followings characteristics [7]:

- *confidentiality*, which means protecting data leaking to unauthorized parties, such as personal identification data or credit card information;
- *integrity*, that suppose to avoid data corruption and keep data integrity;
- *availability*, which means to ensure that data and applications are always available, with any interferences, to authorized entities.

In [8] is considered that the fundamental security requirements on collaborative systems are integrity, confidentiality, availability, non-repudiation, and authentication. Those five characteristics must be analyzed throughout the whole lifecycle of collaborative system.

The banking field is the most exposed to security attacks and the financial losses are significant when security vulnerabilities are found and exploited. The security of banking information systems must be analyzed according to categories of users that accessed them and types of applications integrated in the system. There are some applications of banking information system which can be accessed by internal users (employees) and the others by external users (customers or partners). The access rights and security policies are different, depending on such type of user access. The internal applications can be accessed by employees without many restrictions, respecting the single-sign-on rules. The external applications, which are accessed by customers, such as internet or mobile banking applications have multiple security restrictions, in order to prevent possible security attacks.

4 Ways to Increase the Security through Authentication

In the case of internet banking applications, the users' access is managed by challenge response tokens, which provide passwords that are valid for few seconds and for the requested session.

In order to ensure a high security level inside the information system, the banks have engaged real hackers to test and discover the vulnerabilities of every new application which will be launched in production. The banking informatics applications are exposed to many attacks and it is less expensive for the bank to pay hackers to discover security vulnerabilities than to launch in real environment an application which is not tested enough. In that case, the financial loss for the bank will be bigger [4].

In a banking informatics application only authorized users must have access, based on username and password. The application administrator is dealing with the access rights of each user, adding and deleting some users according with the bank security rules. In order to increase the security level, the application must be protected against SQL injection, so that only authorized users can access it.

The protection against SQL injection is realized by minimizing the letters entered by the user in the textboxes for username and password and by replacing the special characters associated with an SQL statement, as follows [9]:

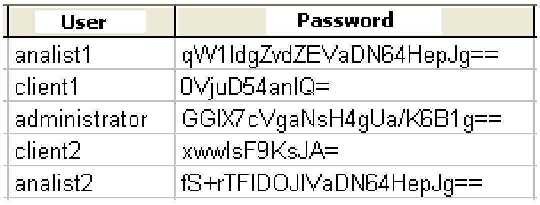
```
string userName =
TextBox1.Text.ToLower().Replace(
"'", "''");
string passWord =
TextBox2.Text.ToLower().Replace(
"'", "''");
```

Another way to increase the security through authentication is to encrypt the users' passwords inside an application. When dealing with data regarding bank customers and details about customers' accounts, every user access must be carefully analyzed and each user must protect its security authentication elements.

The most encounters encryption algorithm used to encrypt the password of every user, so that nobody can read it, even the application administrator, is Triple DES.

The TDES algorithm turns a byte array into an encrypted byte array. First of all, must convert the message string, which is Unicode encoded, into a byte array through the *System.Text.UTF8Encoding* encoder. The key is used to initialize the TDES algorithm. The encrypted byte array is finally converted into a Base64 encoded string for easy storage. The C# TDES code accepts three possible key lengths: 64 bit, 128 bit and 192 bit. Only 192 bit keys are truly TDES, the 128 bit key length obtained from the MD5 hash is only sufficient for Double DES [10].

In Figure 3, a view from the database of a banking informatics application is presented, where the encrypted passwords are stored [9].



User	Password
analist1	qW1IdgZvdZEVaDN64HepJg==
client1	0VjuD54anIQ=
administrator	GGIX7cVgaNsH4gUa/K6B1g==
client2	xwwIsF9KsJA=
analist2	fS+rTFIDOJIVaDN64HepJg==

Fig. 3. View of encrypted passwords

The specific features of banking applications were very important in choosing the best encryption algorithm. The high necessity of securing users passwords was the main criteria in selecting the TDES algorithm, which applies the cipher algorithm three times to each data block.

5 Security inside the System after Authentication

In collaborative banking information systems, the new security elements that must be taken into consideration in the case of electronic banking applications are not related to users' access, because this was already solved. The possible future attacks will be provided by existing users and customers, which will exploit security vulnerabilities of the applications, after they are logged in. These vulnerabilities refer to the possibility to make payments from an unauthorized account or in the name of another user/customer. Taking into consideration that payments are made electronically and in real time, these situations are identified when is too late. The reality gave us different cases when such situations were happened and some banks had significant losses.

Figure 4 present the security vulnerabilities existent in an electronic banking application, after the authentication process.

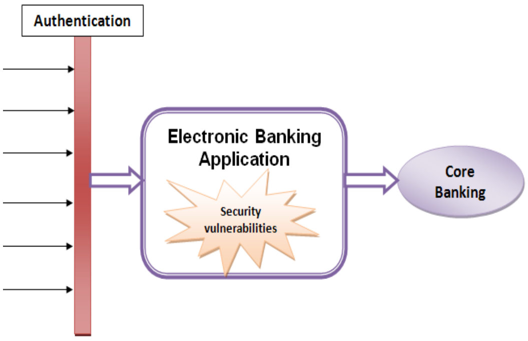


Fig. 4. Security vulnerabilities inside the system

These vulnerabilities must be prevented and eliminated with a sustained effort from the team of electronic banking application developers and administrators. If everyone does his job with responsibility, all the settings will be done correctly and situations such as making a payment from an unauthorized account will not be encountered.

In the case of daily transactions performed in a bank, the characteristics target the workstation, the client account, the beneficiary account and the transaction value. Transactions are sorted by value. Then, are determined the frequencies of the traded amount values and the highest frequencies are chosen. It is verified if the transactions were made from the same workstation. The persons who operated the transactions are identified. The traded amount beneficiaries are determined. From the analysis, abnormal situations arise, meaning that all transactions were made to a certain destination or all transactions were made from the same workstation [11].

6 Security outside the Authentication

In [12] is considered that most existing collaborative systems utilize a username and password to authenticate users. If the systems are not integrated with other systems, these credentials are unique for accessing all systems resources and must be delivered to the end users. The distribution of these credentials to the end users is not always properly secured, which means that they can be intercepted during the transmission by a person who could use them to gain unauthorized access to the collaboration.

In the banking information systems, there are some applications that do not require users' authentication. Generally, these applications are accessed internally, by the bank employees, and the access is provided from other applications, based on single-sign-on principles. In such situations, the security must be ensured through restricted access rights on mainly resources and by monitoring users' access with the help of log files.

Security outside the authentication means that users can easily approach to the system, without any authentication procedure. Unauthenticated users can enter into the system, modify the data and use system resources. Security vulnerabilities that appear in a collaborative system, outside the authentication, refer to malicious users that could enter into the system, observe and interact with participants [9-8].

In [13], processes for security optimization are presented, in which the collaborative aspect generates new features regarding their acceleration.

7 Ways to Increase the Security in Collaborative Systems

One of the ways to increase the security level in collaborative systems is represented by the use of roles to ensure the confidentiality of messages within the system applications. Each user has a unique role that provides specific access rights to certain resources.

The matrix of roles highlights the user access rights within the systems applications. There are messages that are available to some users and messages that are visible to the others. Access rights are set at both homogeneous group of users and at the level of the individual.

Another way to increase the security inside collaborative systems is given by backup procedures of databases and applications. Each bank has well tuned procedures for backup and disaster recovery, to avoid the loss of database records, even for natural disasters events.

Databases with transactions performed in a bank contains information about the user who performed the operation, the channel through was done, from which workstation, in which date and which hour. These databases are updated in real time and are consulted by the Banking Security Department to discover any fraud attempts. If someone found that, from a workstation, an operator makes a lot of transactions compared to other operators, or amounts transferred are very high, then an investigation is made regarding these operations [11].

8 Conclusions

The security of collaborative systems is a very important quality characteristic that must be analyzed in detail to ensure a high security level inside such kind of systems.

The security of collaborative systems must be treated independently from other important characteristics, such as *concurrency*, which means providing simultaneous access to shared resources, and *transparency*, meaning that the various operations taking place between components are typically hidden from the end user, which actually perceives the system as a whole.

References:

[1] A. Crabtree, *Designing Collaborative Systems: A Practical Guide to Ethnography*, Springer Publisher House, 2003.

[2] R. Babuška, F. Groen, *Interactive Collaborative Information Systems*, 1st Edition, Springer, 2010, 595 pg.

[3] S. I. Nitchi, A. Mihăilă, M. Podean, Collaboration and Virtualization in Large Information Systems Projects, *Informatica Economică Journal*, Vol. 13, No. 2, 2009.

[4] C. Ciurea, The Development of a Mobile Application in a Collaborative Banking System, *Informatica Economică Journal*, Vol. 14, No. 3, 2010, ISSN 1453-1305.

[5] C. Ciurea, *Metricile sistemelor colaborative, PhD Thesis*, Bucharest University of Economic Studies, Bucharest, 2011.

[6] E. van Ommeren, S. Duivestein, J. deVadoss, C. Reijnen and E. Gunvaldson, *Collaboration in the Cloud*, Microsoft and Sogeti, Netherlands, 2009, pp. 122, ISBN 978-90-75414-24-0.

[7] P. Pocatilu, M. Doinea, C. Ciurea, Development of Distributed Mobile Learning Systems, *The 9th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing (CSECS '10)*, Vouliagmeni, Athens, Greece, December 29-31, 2010, ISBN 978-960-474-262-2, ISSN 1792-7315, pp. 196-201.

[8] Yuseung Sohn, Hyun-Yi Moon, Seunglim Yong, Sang-Ho Lee, Security Issues of Collaborative Review System, *Fifth International Conference on Information Technology: New Generations, ITNG 2008*, 7-9 April 2008, pp. 581-586.

[9] C. Ciurea, Implementing an Encryption Algorithm in Collaborative Multicash Servicedesk Application, *Open Source Science Journal*, Vol. 2, No. 3, 2010, ISSN 2066–740X.

[10] Encrypting and Decrypting a C# string, Available at: http://www.dijksterhuis.org/encrypting-decrypting-string

[11] I. Ivan, C. Ciurea, S. Pavel, M. Doinea, Security of Collaborative Processes in Large Data Sets Applications, *The 5th International Conference on Applied Statistics*, November 19-20, 2010, Bucharest, Romania, ISSN 2069-2498.

[12] E. Hladka, D. Kouril, M. Prochazka, L. Matyska, P. Holub, Transparent security for collaborative environments, *International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2007, CollaborateCom 2007*, 12-15 Nov. 2007, pp. 79-84.

[13] M. Doinea, *Optimizarea securitatii aplicatiilor informatice distribuite, PhD Thesis*, Bucharest University of Economic Studies, Bucharest, 2011.