

Security Process Development in Collaborative Systems

Mihai DOINEA
Informatics Economics Department
Academy of Economic Studies, ASE
Bucharest, Romania
mihai.doinea@ie.ase.ro

Abstract: *Collaborative systems are presented and classified. Security aspects are presented regarding the maintenance of quality characteristics. Collaborative security problems are discussed and ways of applying it are debated. Security process is implemented in a case study presented. All the aspects discussed take security aspects and implements them into the collaborative processes discussing the main correlations.*

Keywords: *security, collaborative, systems, process, characteristics, quality*

1. Collaborative systems

Everyone knows that every day of our life is an interaction with hundreds, maybe thousands of extern factors. The world in our days, in this knowledge based society had grown smaller. Distances have been shortened. All can interact with no difficulty, with people that are at thousands and thousands miles away, by means of complex network systems that have been implemented in the latest decades. This collaboration between all kinds of informatics systems had given us a chance to see the world much easier than in the past. Every day problems are now much easier to deal with and for that we are more effective in our work.

The collaboration is a characteristic of intelligent behavior encountered in any work undertaken. The simple fact that we are social beings makes collaboration to be part of our every day life.

We can say, in conclusion, that collaboration has come to support the well known idea which says that: *two are better than one, always.*

Collaboration has entered in the IT area, as the collaborative system concept. Collaborative systems coordinate collaboration among multiple users who are fulfilling common tasks over computer networks, increasing productivity and lowering costs. Almost, every work field has a type of collaborative system. As presented in [01] there are many criteria for collaborative systems classification. An essential one is the application criteria, after which collaborative systems can be divided in:

- collaborative systems in education;
- collaborative systems of defense;
- collaborative systems in production;
- collaborative banking systems.

Another criteria of classification of collaborative systems is the organization criteria. In [02] is presented the following classification criteria, after organization structure:

- linear – figure 1, initial entries are I_1 and final outputs are O_n ; at intermediate levels, the outputs of k-1 subsystem are the entries for k subsystem; these types of

collaborative systems are encountered in the field of education, each subsystem representing a graduate school;

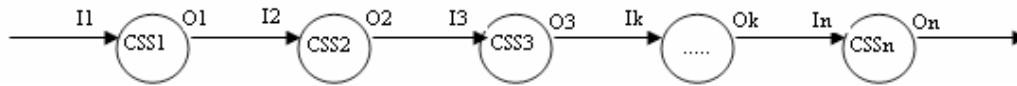


Fig. 1. *Linear structure*

- arborescent – here messages move between subsystems in hierarchical sense, that means a message from the level two will reach the top level only if it passes first to the level one; in the example shown in figure 2, each subsystem has many entries and many outputs and the information flows move in both directions; the information flows exchange can be done also on the same hierarchical level, in the given example between *CS11* and *CS12*; systems of this kind meet in organizational management and public administration; considering the collaborative system as a tree structure, there are taking into consideration:
 - the degree of vertical collaboration as the number of links between components from level k to the ones on level $k+1$;
 - the degree of horizontal collaboration as the number of links between components on same level.

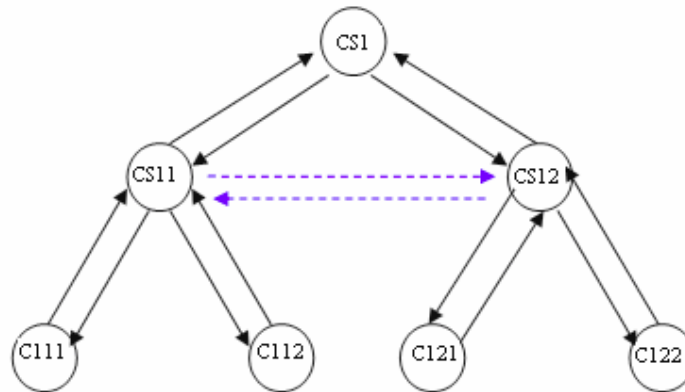


Fig. 2. *Arborescent structure*

- network – subsystems are all interconnected, that all transfers are interrelated, messages circulate between all components without any restriction, figure 3; network type collaborative systems meet in the field of production and banking.

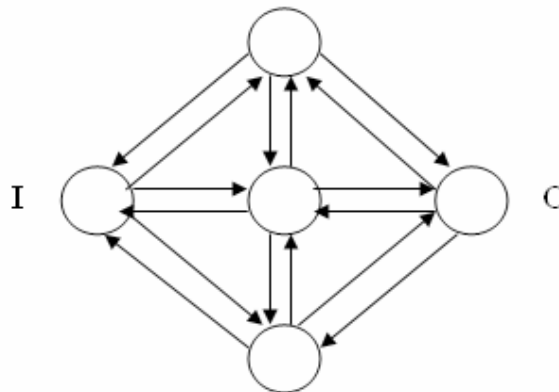


Fig. 3. *Network structure*

A collaborative system is an open environment where users are interacting in a shared activity, from remote locations. Collaborative systems are a part of distributed applications in which users are working together towards a common goal.

2. Security concerns

Security is defined as the ability of a system to resist malicious attacks that could compromise the main characteristics of data.

Concerns are given by the communication intensity which in collaborative systems is very high. And other characteristics must be kept in order to have a strong, reliable system but the communication is vital in keeping unchanged the main characteristics of information:

- authenticity – is the characteristic that can tell if the message that has travelled through the network and came to destination is the original one who has left the expeditor; authenticity is achieved by digital signing the message with the sender private key;
- integrity – integrity represents the assurance that data is complete and accurate, especially after it has traveled from one point to another in its collaborative system workflow, and possibly been read by many small intended users; integrity must be maintained to prevent tampering with the data, and is usually achieved by adding a checksum to the end of the message as a hash function;
- confidentiality – is the assurance that a message has not been read by anyone other than the intended reader; confidentiality is often provided by the encryption of data using a public key/private key scheme;
- non-repudiation – has been added to prevent the owner from rejecting messages that he create and signed; it's an indivisible bound between the composer and digital content which can't be broken by any means.

To understand those concepts in the context of collaborative systems we must analyze the main characteristics of them to determine in which degree they keep unchanged the information.

According to [03] collaborative systems characteristics are:

- complexity – is a measure for the interdependencies between components and their links and also for the diversity of different types of input and output constructions; this characteristic describes the density of fluxes between the components of the system; the complexity of the collaborative system generates a large number of various components; based on that, a proper approach of the system quality is to analyze every component separately;
- reliability – the system *reliability* is determined by analyzing the number of problems solved by the system and the total number of specified problems;
- maintainability – is a process particular to software products that have a complex development process and that are intended to be used for a long time, meaning more than three years; in this category are included also products like the collaborative systems; maintainability measures the effort needed to make modifications on the collaborative system in order to make it suited for current needs; this effort can be described as consumed time, number of modules modified, number of added modules and number of deleted modules;

- functionality – describes a set of functions and their specified properties; functions must satisfy the declared or implied need;
- usability – defined by the ability of a system to be useful for his agents; usability of a collaborative system is reflected through the effective interactions between its agents and the successful achievement of proposed objectives;
- stability – is the characteristic that reflects the interdependence between the large number of entities from which a collaborative system is composed; this characteristic must be preserve as a prior condition for the reliability.

A collaborative system has to be able to assure all the security quality characteristics otherwise the losses could be extreme. For this, accordingly to [04], organizations must:

- keep the system and its services up and running all the time, excepting periods when backups or updates are made;
- verify all the connections made to the system;
- assuring that users privileges are correct;
- provide trustful information to all its stakeholders;
- protect sensitive information by means of cryptography;
- keep logs of every transaction made on the system.

Security in the current knowledge based society it's a must which shouldn't be forgotten in each and every project development stages.

3. Collaborative systems security aspects

As the main data characteristics presented above must be preserved, the communication in a distributed collaborative system must be a priority given the multiple and simple attacks that could interposed in the communication process.

Traffic analyzers could simply determine the nature of data transmitted and intercept all information on various ports and protocols.

In the following example presented in figure 4, is presented an interception of a query request from an Oracle server – *select * from answers.*

No.	Time	Source	Destination	Protocol	Info
2	0.001260	86.55.177.71	10.2.6.231	TCP	4365 > pciarray [A]
3	0.001297	86.55.177.71	10.2.6.231	TCP	4365 > pciarray [P]
5	0.001338	86.55.177.71	10.2.6.231	TCP	4365 > pciarray [P]
1	0.000000	10.2.6.231	86.55.177.71	TCP	pciarray > 4365 [P]
4	0.001317	10.2.6.231	86.55.177.71	TCP	pciarray > 4365 [A]
6	0.179076	10.2.6.231	86.55.177.71	TCP	pciarray > 4365 [A]

Stream Content:

```
.Z.....1.....A...!.....
.....2.....select * from answers.....
```

10.2.6.231:pciarray --> 86.55.177.71:4365 (90 bytes)

File: "C:\DOCUMENTS\ADMINI~1\LOCALS~1\Tem... | Packets: 6 Displayed: 6 Marked: 0 Dropped: 0

Fig. 4. Oracle Query Request Capture

Applying filters will reveal all the traffic on all ports from all protocols that an attacker is interested. This kind of attack is ranked as a passive one, its goal being to have access to information without compromising it directly. But this kind of attack is just the precursor of active attacks that could damage entirely a distributed collaborative system.

It can be seen from the figure 5, that the actual information is transmitted along with the table structure which represents a highly vulnerability of a distributed collaborative system. The table structure is composed from the following fields:

- idanswer;
- idquestion;
- iddetail;
- questiontime.

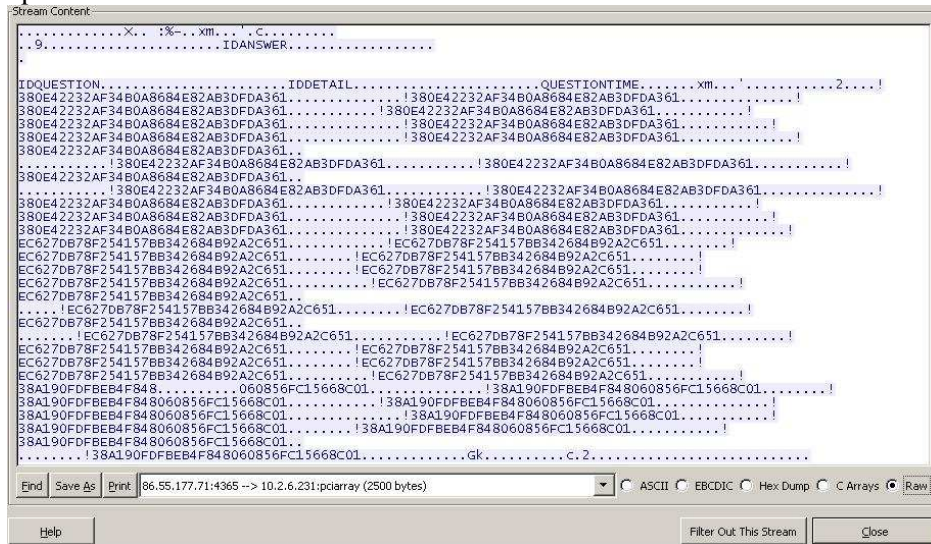


Fig. 5. Captured Oracle Query Results

All data can be viewed in different format types like:

- ASCII – *American Standard Code for Information Interchange*, represents a character codification system based on english alphabet;
- EBCDIC – *Extended Binary Coded Decimal Interchange Code*, is an 8 bit character encoding used on IBM systems;
- Hex Dump – represents a hexadecimal view of data;
- C Arrays – an array view of data;
- Raw – raw view of data.

Collaborative systems’ users must decide whether or not to secure communication traffic on the network. This situation must be carefully analyzed in the context of optimization because securing network traffic has disadvantages on communication performance.

4. Security process implementation

Process optimization is a very debated subject in many fields of technical interests. The optimization has entered the security area under many different aspects. One, which is important for majority of the organizations, is the security optimization criteria under the aspects of security costs. This optimization is considered to be, for the top management, a

tuff decision which must be made using security specialists under a very strict evaluation of vulnerabilities and risks.

Vulnerability, [05] is classified after the level it appears in:

- information vulnerabilities – due to inconsistent of source code many information can be offered to the attackers;
- physical vulnerabilities – defined as vulnerabilities which can exploit the main frame in which open source products are running to gain access to resources;
- processing vulnerabilities – given by the usage of untested instructions or processing sequences;
- communication vulnerabilities – due to bad implementation of communication protocols or to different forgotten aspects of communication.

Risk is defined as a threat that exploits the vulnerabilities in collaborative systems. Will be considered the following categories of risks, classified by potential source:

- risks due to uncontrollable events like natural disasters, external agents;
- risks due to political or economic circumstances;
- risks arising as a result of technical or technological problems;
- risks due to human behavior, lack of training of staff that works with distributed systems.

In [01] is presented the following collaborative banking process which will serve as an example for the optimization security process. It is a collaborative banking system in which a collaborative process takes place. In this frame are four departments that interact for resolving the clients' requests. In figure 6 is presented the work flow for this collaborative process.

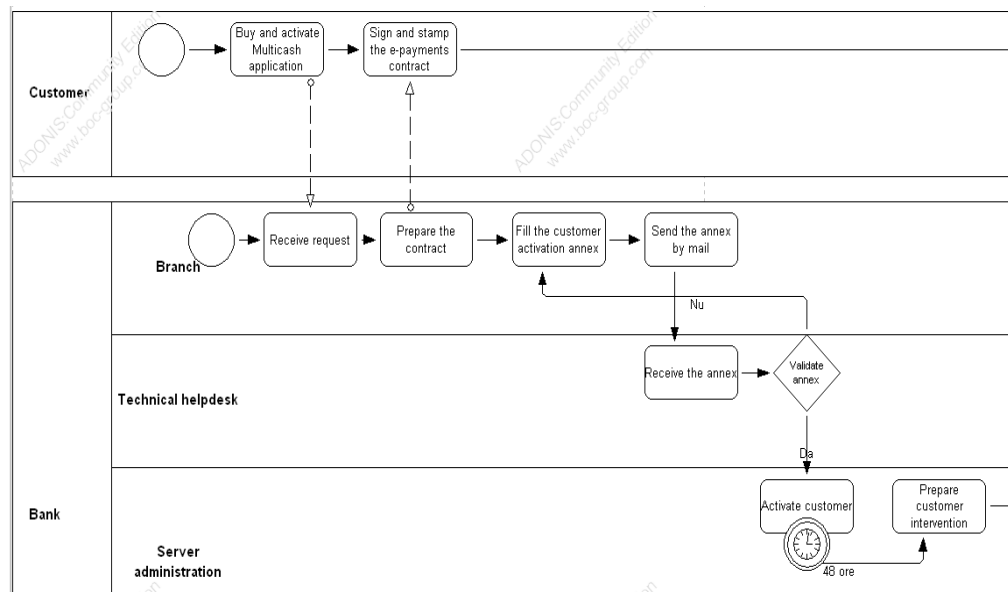


Fig. 6. Collaborative banking business process

The four entities are as follow:

- branch;
- technical helpdesk;
- server administration;

- intervention.

In the collaborative banking business process presented in figure 6, the customer and the bank must cooperate in order to achieve their goals, meaning that customer receive the wanted service and the bank conclude a contract in its advantage. If the customer wants to make electronic payments, he must buy and activate the Multicash application. For doing this, he will sign and stamp an e-payment contract. The bank branch will receive the activation request, will prepare the contract, fill the customer activation annex and send it via mail. The bank technical helpdesk will receive the customer annex, validate it and if everything is in order, the bank server administrators will activate the customer and prepare the intervention for installing the application.

This is a collaborative process in which many agents work after strict rules and procedures. If an agent will do a mistake, everything will be destroyed.

So, what's the purpose of this collaborative banking business process presented in [01] if after all stages had been completed, at the last one, someone doesn't do his job correctly? Here comes the part in which security process optimization step into. The purpose is to have a collaborative business process flawless at the end. This is achieved using a fail-safe or a fail-secure security process, meaning that in the event of a process failure another process will come in and do something about it.

Fail-safe is different from fail-secure. In the first case, if an event of a collaborative process failure had happened, a fail-safe procedure doesn't do anything about it in the system just alerting the authorized personnel about the failure but allowing it any actions to be taken either correct or not. The second one, fail-secure procedure alerts the authorize personnel and blocks all the actions that normally would follow the failed one. Actions that could follow in case of a collaborative process failure are:

- freeze the process until someone qualified to deal with will resume it;
- try to repeat the action and blocking it after several failed attempts;
- passing to the next one but writing a report at the end of the workflow;
- attempting to execute all process with any action undertaken.

Based on the collaborative banking business process presented above a new collaborative banking frame is developed which will include a security frame under which operations take place and a fail-safe or fail-secure security process which control the execution of the entire workflow. This new work frame is presented in figure 7.

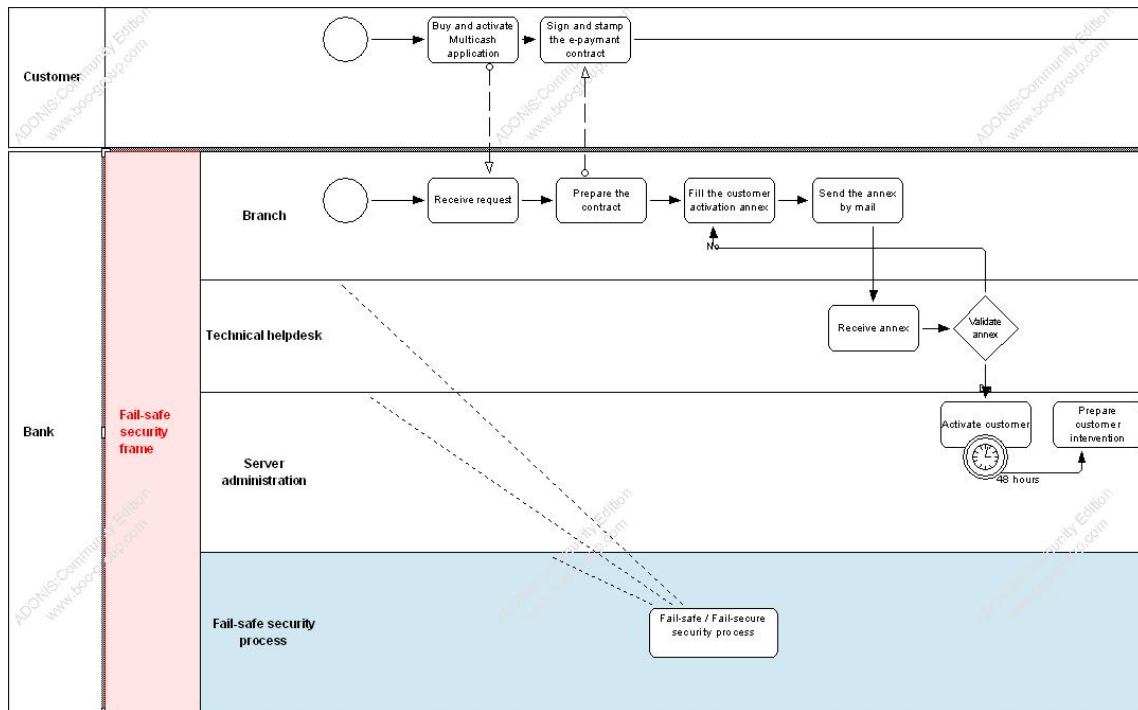


Fig. 7. Collaborative banking business process secured

Using different security models a fail-safe process could be implemented to reduce losses and personnel implied with the workflow process. Instead of having at least an agent for every level of the workflow, a security process will manage all the activity and report problems found to a single qualified agent.

5. Conclusions

Collaboration was always an important aspect of our life even if we know or not. In the IT&C area collaboration is more important because informatics systems represent now a huge dependence without which our work wouldn't be so efficient.

In the current society where communication is vital and information represent the added value of someone's work, collaboration must be encapsulated in a protective shell represented by the security methods and techniques.

From collaborative systems to collaborative society the security aspects must be treated carefully.

References

- [01] C. Ciurea, M. Dumitrache and M. Doinea, "Distributed Collaborative Systems Security," *Proceedings of Knowledge Engineering: Principles and Techniques Conference (KEPT) 2009*, July 2-4, 2009, Cluj-Napoca, Romania, Special Issue of Informatica Studia Universitatis Babes-Bolyai, Vol. 54/2009, Cluj University Press.

- [02] I. Ivan, C. Boja and C. Ciurea, *Collaborative Systems Metrics*. Bucharest: ASE Publishing House, 2007.
- [03] I. Ivan and C. Ciurea, "Quality characteristics of collaborative systems," *Proc. The Second International Conference on Advances in Computer-Human Interactions*, vol. I, Cancun, Mexico, IEEE Xplore Digital Library, 2009, pp. 164-168.
- [04] M. Doinea, "eBusiness security architecture," *Informatica Economica Journal*, vol. XIII, no 1/2009, pg. 137
- [05] M. Doinea, "Open Source Security – Quality Requests," *Open Source Science Journal*, no. 1, Bucharest, 2009.
- [06] I. Ivan, M. Doinea, S. Pavel and S. Vinturis, "Security management in distributed IT applications," *The Proceedings of the Ninth International Conference on Informatics in Economy, IE 2009*, May 7-8, 2009, Bucharest, Romania, ASE Printing House.
- [07] I. Ivan, C. Boja, C. Ciurea, R. Enyedi, C. Toma and M. Popa, "Collaborative Systems Metrics," *International Workshop in Collaborative Systems*, Cluj-Napoca, October, 2006.
- [08] D. Stevenson, M. Hutchins, C. Gunn, M. Adcock, A. Krumphols, *Multiple approaches to evaluating multi-modal collaborative systems*, CSIRO ICT Centre, Australia, 2005.
- [09] C. Ciurea and B. Zurbagiu, "Virtual campus collaborative learning and its security," *The Ninth International Conference on Informatics in Economy*, Bucharest, Romania, 2009
- [10] T. Daradoumis, F. Xhafa and J.M. Marques, "A methodological framework for project-based collaborative learning in a networked environment," *Int. J. Cont. Engineering Education and Lifelong Learning*, vol. 12, no. 5/6, 2002

Author



Mihai DOINEA attended the Faculty of Economic Cybernetics, Statistics and Informatics of the Academy of Economic Studies, graduating in 2006, Computer Science specialization. Having a master degree in Informatics Security, promotion 2006-2008, he is currently a PhD candidate, Economics Informatics specialty in the same university, also teaching as assistant to Data Structure and Advanced Programming Languages disciplines. Following are the fields of interests in which he wrote a number of papers in collaboration or as single author concerning: security, distributed applications, e-business, security audit, databases, and security optimization.