

Social Networks Security

Ion IVAN, PhD

Department of Economic Informatics
Academy of Economic Studies, Bucharest, Romania
ionivan@ase.ro

Mihai DOINEA

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

***Abstract:** The concept of social networks will be presented with emphasis on web portals. Security requirements for such network communities will be analyzed and the necessary components for assuring a safe level of security will be presented. An efficient and safe environment for collaboration in such communities will be described and a comparison with the way in which is actually implemented in a real social network is conducted.*

***Keywords:** social networks, security, collaborative systems, web portals.*

1. Social Networks and Web Portals

Knowledge based society had brought new exciting features for improving our life quality. From the largest scale used, mobile device, up to the most web used, social gathering places, the knowledge based society changed our way of acting. Our primitive means of communication were transformed, in this way narrowing the distances and enhancing the speed of communication. What, in the last decade seemed to be a science fiction set up, had reveal itself to be more touchable, being used by many users even in the most third world countries.

Many of us consider this feature as being a constructive and useful way of interacting, changing information, working together towards a common goal, helping others and enjoying in a completely new and *unlimited* environment. The possibilities are almost literally infinite, because any kind of relation between two parties can be imagined and actually implemented and only the IT&C hardware and software aspects could put some breaks in the process, but today's technologies are very developed, so the only impediment would be that of our capacity of imagine and designing those systems.

We have seen how knowledge-based society is developing with its Web tools and all the information enrolled in their process, how independent users can express themselves through a wide spectrum of applications that do not need programming skills. But what is happening from an organization perspective, how this way of going thing is affecting the organization status. It is a good way or a bad one?

If we consider that every user is also a part of the organization entity, then we can definitively say that the organization position is altered in some way by the users' actions. If users share their knowledge in these high, interrelated communities than their knowledge could contribute to other organization well being or to their own organization, depending on the content that they provide to others.

Knowledge means power; whoever has it can rule on the blackboard. So if you share something on the Internet, than you shouldn't rely on their value because anyone can see it and even use it against you as it is presented in [1]: "People believe that if it's their

information, it belongs to them. Wrong. On the web, whatever you've posted, it doesn't belong to you anymore.” Having this fact known, organizations must take seriously into consideration the following questions when they decide to share information or when their employees decide to undertake such actions:

- what kind of information do they share; is it vital for the organization or is it just for common public use?;
- where they share information; on which systems organization decide to put information for sharing it?;
- when they share; the time is it related to an important event or it is not a crucial knowledge and the time doesn't matter?

Regarding their employees, organizations must define work policies in which they must specify the confidentiality aspects of their employees' related work.

The social networks provide a huge opportunity for implementing collaboration between users or different processes and actions undertaken by users. In this way a huge benefit could be brought to the community but as well, real threats could emerge, because a good think always has a high price to pay.

2. Security aspects and characteristics of web portals

There is no question whether or not the security aspects must be a priority for an organization. The issue of content security, which eventually means knowledge, must be a top priority throughout any organization infrastructure, starting from CEO and ending with the most insignificant worker in the enterprise.

Organization must decide whether or not to outsource its security aspects to another party under a very well founded undisclosed agreement. This decision must be taken after a very good evaluation of its benefits and drawbacks.

But security solutions are hard to find, even though their number is increasing rapidly. Why? Because of the unique pattern assigned to each and every organization. Every enterprise has its unique configuration and requirements, so the security solution must also be unique to comply with the organization's demands. These aspects could sometimes be hard to get and the budget for security concerns could increase rapidly. Even so, companies seem increasingly dedicated to provide financial resources for such needs, understanding their need of visibility but which comes with a higher price to pay. But this it wasn't the case couple years ago when, for example, encryption, it was just a “nice to have” feature.

As social networks rely on distributed platforms, implicitly they inherited the security issues that arise in a distributed scheme. So, all the security aspects must be preserved for such network collaborative groups could work properly.

Following lays the main aspects that a distributed platform should implement in terms of security for such social networks:

- the way connections are made to the main interface; whether they are secure, if they are using trustful authentication schemes, if they can manage the non-repudiation aspect of every action unrolled on the platform;
- the way communication is managed inside and outside the collaborative application; if integrity and confidentiality demands are met using hash functions and encryption schemes; either if organization uses a virtual private network or if information is travelling freely on the Internet;
- the way additional processes can be added to the initial set up of the system on a safe and easy fashion without upset the level of reliability and efficiency.

The security characteristics for a social collaborative network are to be discussed regarding the implications that they have on the scalability characteristic of the system in subject. Because of the fact that such kind of networks implies many users that come with their knowledge base, the security characteristics must heavily be implemented based upon the scalability characteristic. Those being:

- confidentiality – the security characteristic of information which can be scrambled based upon a symmetric or asymmetric cryptographic algorithm in order to be viewed only by those who know the encryption or decryption key, depending on the type of algorithm being used;
- integrity – the characteristic of information which reflects that a data was changed or not in a communication process; this characteristic can be assured using one way functions, e.g. SHA1, MD5, etcetera;
- authenticity – it regards the right for using a certain services available in a collaborative system, services that are designated only for private use;
- availability – shows how a collaborative system treats data that are transferred in its process, in such a way that they always should be there when someone requests for them.

If we look upon the web portals we can say that the information is treated as if security would mean only certain aspects of the ones presented above. So, some of collaborative systems consider that by having a strong authenticity procedure will resolve the problem of having integrity or confidentiality, which is absolutely false. One aspect doesn't involve another and there are many examples of good or bad practice.

Social networks in which knowledge is a vital fluid must undertake all the procedures that are necessary for creating a safety and helpful environment without having to lower the following characteristics:

- usability – the capacity of the collaborative system to be used by as many types of users without difficulty; is the characteristic of being intuitive and can be measured through:

$$IU = \frac{\sum_{i=1}^n (1 - p_i)}{m},$$

where:

IU – usability indicator;

n – number of successful operation with or without assistance;

m – number of total operations;

p_i – percentage of assistance as part of the entire process.

- reliability – the collaborative application is meant to work whenever, wherever and on whatever system a user is operating on and can be defined as:

$$IR = \frac{NSI}{NTP},$$

where:

IR – reliability indicator;

NSI – number of successful iterations;

NTP – number of total processes.

- accessibility – due to the normative set up defined by the European Union, every public system must have implemented a variety of tools which should help normal people but also people that have different kinds of disabilities; this creates a competitive stage for other systems; the accessibility can be measured using the following indicator:

$$IA = \frac{NSDCP}{NDCA},$$

where:

IA – accessibility indicator;

NSDCP – number of successful digital content processed;

NDCA – number of total digital content accessed.

These characteristics refer to the final user satisfaction and are meant to increase the level in which a user, after having accessed such a system, could say that was truly satisfied and didn't encountered any problems in resolving his issues.

3. Security components in web portals

For assuring a higher degree of security to this types of applications we must, first, understand well how they are working, what are all the links that could be made through these applications, basically what are the connections between the application and the possible sources of threats.

Regardless of where a threats originates, from inside or outside the system, always exists measures that can deal the problem, offering even a number of solution from we can chose accordingly to our budgets, our need of security, our expectations.

Following are unfolded a list of security measures and components [1] that can be used for protecting the need of privacy or the integrity of a collaborative system:

- technologies for analyzing the code when it is written and detecting the potential security vulnerabilities;
- methods and techniques for monitoring, controlling and preventing leaks or from detecting possible attacks through which information could escape;
- solutions for determining the main programs that run without the latest patches or which program can run and which not, based on a risk assessment, determining the possible vulnerabilities;
- solution for data protection; the protection of data integrity or the characteristic of privacy; data back-up policies and data recovery systems;
- data risk management solution for determining who's using data and for what purpose;
- solutions for identifying abnormalities inside the system like: viruses, different hijacking tools used on the processes that run on the system, flood attacks that could bring down the system or even DoS, Denial of Service attacks which are more frequent;
- strong and reliable security policies with concern to: the physical area in which the system is functioning; the list of privileges an authorizations for every user that can access the application's services.

For understanding better the need of security and identifying correctly the security components that should be implemented, first we have to determine how the system is interacting with the outside world via his inside functionality. Following is presented the SWOT analysis for a web portal collaborative system, figure 1. The blue zone is representing the inside aspects of the system good or bad and in the red one are represented the outside aspects which could have positive or negative influence on the system. The green points are the strong parts of the system coming from inside and outside. The olive points underline the main deficiencies found on the inside but also coming from outside.



Fig. 1. SWOT Analysis for Web Portal

A SWOT analysis could be conducted to identify all the connections from inside and outside the collaborative area, in this way estimating in a simple fashion the possible costs that could arise in case something is not working well. Doing so the following aspects could be identified:

- strengths – all the inside hard points that such systems can have like: they implement content security, they provide confidentiality to third parts, they use strong authenticity procedures, etcetera;
- weaknesses – all the inside disabilities that could be identified: uninstructed personnel, deficient network infrastructure, improper hardware equipment, etcetera;
- opportunities – all that exists outside of the system and can be used in its advantage: a wide internet network that reaches millions of users, different means of attracting users and promoting the business, a high and well founded development tools for creating almost all we can imagine;
- threats – all that exists outside of the system and could mean a treat to the good health of the system: millions of computer viruses that could affect the machines that support this kind of services, thousands of hackers that could access the files, break into the system, modifying or stealing information, so decreasing the level of credibility in such collaborative systems.

4. Safety environment for collaboration

A safety environment for collaboration represents a set of rules that such systems must implement in order for a proper and natural activity can be sustained. These types of rules could be anything from a simple working procedure regarding the activity of a collaborative system up to well defined security policies and management acting towards this goal. A safety environment for collaboration also means to create a reliable connection between the system and its processes and all the actors with which the system could interact. If such a collaboration system is launched into production in places that are known to be unstable and a

proper security policy isn't implemented to contra attack the main risks at which the system is exposed then the whole collaboration thing could lead to various unpleasant results.

A collaborative system must always address communication aspects as being a top priority. The fact that these systems encapsulate all the aspects and technologies related with communication as IM, email, web portals, social network, open source communities, different systems for correlating each person's work, they must pay attention to all communication processes that are part of the system.

The means for creating a safety environment for collaboration inside of an organization who want to use this kind of systems is by implementing a well defined security policy. An organization has to get into consideration the following aspects:

- defining a rigid security policy which must be implemented at all levels of the organization;
- a detailed analysis of all the organization assets ending with a report which must specify every asset, value and its vulnerability issues;
- assuring security by instructing every employee with regards on their roles and responsibilities, how they can access and use the hardware equipment and software programs, if necessary, doing trainings about the security issues;
- defining security measures regarding the physical areas where hardware equipments on which the collaborative systems run; securing all the hardware components from unauthorized access, possible mall functions due to the improper use;
- implementing security at the most important level of the system which will be communication level; using controls for protecting against malicious programs from outside the network and using back-up systems for safety precautions;
- using monitoring systems for tracking information flow throughout the network and even outside the organization area; logging all the operations that presents security vulnerabilities in order to detect rapidly any kind of attack passed through that process;
- access control should be carefully defined as users must manage various types of resources; in this way an organization who's implementing such collaborative systems should manage the access on the following levels: operating systems, databases, networks and applications through rigid user access management policy;
- rigorous maintenance process for the purpose assuring the efficiency and performance of every software solution implemented in the system;

A rigorous workflow must be created for sustaining all the process that need to interoperate in order to provide access to the collaborative resources. When collaborative systems began to be fully operational, having thousands of users, then any change in the system's architecture is difficult to be implemented if the system wasn't rigorous design in its beginning. A new process added in the main workflow can be a really difficult problem to overtake with really big losses regarding the operability of the system. In [2], figure 2, is presented an architecture to develop an agent-based workflow management system for collaborative product design.

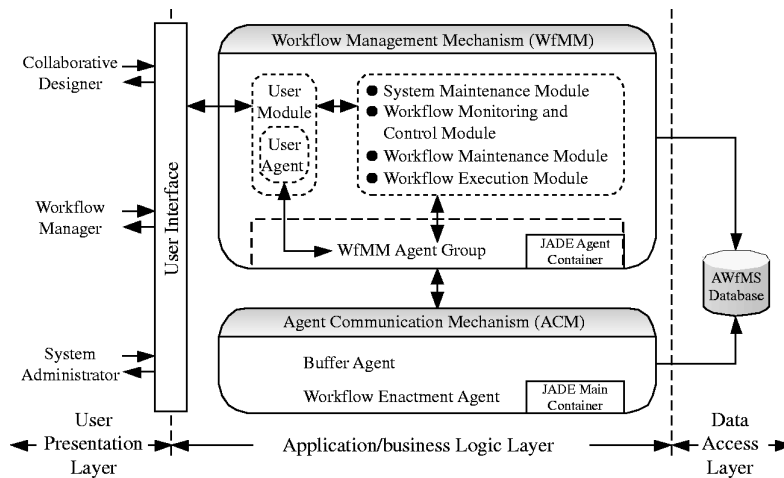


Fig. 2. Collaborative product design

Sometimes the difference between a good and a bad, an efficient and a nonperforming collaborative system is made in the process of designing it, regardless the resources that were thrown in the process of building it.

5. Description of a social network

A very well known business oriented social network which present passes over 50 million registered users worldwide, is LinkedIn founded in December 2002 and launched in May 2003. Most people are using LinkedIn for *getting to someone*, in order to make contact with that person for different purposes. The possibilities that LinkedIn is offering to its users are:

- increase the visibility by adding new connections to user's profile and by providing all the details necessary for completing it; connectivity is improved and possibilities of making even new connections are increased;
- improve Google Ranking for searches about user's profile by making the profile to be fully visible by the public and adding public references to the personal web page, if it's available;
- understand the evolution of certain companies which might be relevant for later user's career;
- integrate new widgets tools and export content into other applications;
- answer and receive answers at questions relating companies and user professional interests;
- posting all user's past activities and future perspective;
- developing user's business by making new connections, doing marketing research in terms of the products.

LinkedIn resources are intended for the use of the following categories of users who for achieving their goal must have a dynamic activity:

- people new to the network who entered for the scope of get help in their business or career;
- people who want to met new friends or colleagues and extend their knowledge in the business they're into.

For this social network an analysis will be conducted concerning the main security aspects which were identified in the functionality of this social network. If consider the

communication as being an important part of the collaborative process then we should analyze some aspects regarding the quality of the communication for the LinkedIn network.

The security aspects will be conducted for the following characteristics:

- users authenticity and the authentication process;
- information confidentiality;
- non-repudiation aspects of user’s actions;
- integrity concerns.

The authenticity of users in the LinkedIn application and the authentication process are the main instruments for assuring the security. These processes are implemented through means of OAuth which is an open protocol to allow secure API authorization.

The process of authentication is securely managed by using secure a connection through HTTPS protocol as can be seen in the figure 3, in which is presented the URL string for connecting to the application and as well intercepted traffic packets that reveal the fact that an encrypted handshake protocol is implemented.

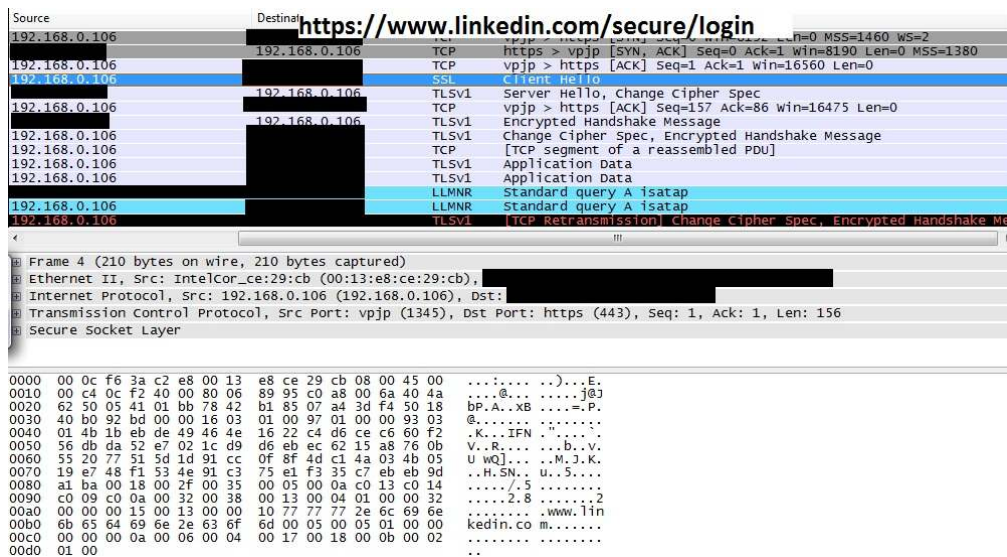


Fig. 3. Packet interception on authentication process

The information processed after the moment of authentication could or not be encrypted depending on the sensitivity and the desire of confidentiality that a user wants.

Having a session token, users can’t deny their actions and every single process undertaken in the system can be assigned to a user uniquely.

An important aspect is the one of information integrity which must be a priority for all sensitive data found in the system. Using a traffic analyzer, communication between user and LinkedIn reveals that not all the data is encrypted, and some information could be intercepted as raw data in the network by anyone who knows how to use such kind of tools. But these information are part of the user’s profile which otherwise can be accessed by anyone from the LinkedIn site. All information related to the user’s privacy is securely managed through a HTTPS connection.

6. Conclusions

As more and more collaborative systems arise for helping users connect to each others, the more, idea of security must be seen as a *must* for offering reliable services and trustful applications to the users.

Collaboration tend to be an important aspect of user's lives and the need of shorting the distances just for sending a message or chatting with someone, or experiencing together with the loved ones multimedia content, or trying to resolve important business issues that are relevant for an organization, is becoming more and more frequent and appealing.

The XXI century user is found in a new and surprising posture, that of a man who must accept the new technologies as part of their daily life but also trying to struggle in the fight for expressing themselves and getting a unique identity in a world where identity is synonymous with the anonymity found behind their computers.

Acknowledgements

This article is a result of the project „Doctoral Programme and PhD Students in the education research and innovation triangle”. This project is co funded by European Social Fund through The Sectorial Operational Program for Human Resources Development 2007-2013, coordinated by The Bucharest Academy of Economic Studies (project no. 7832, “Doctoral Programme and PhD Students in the education research and innovation triangle, DOCECI”).

References

- [1] M. McClure, “Creating Safe, Collaborative Cultures in a Web 2.0 World,” in *EContent*, June, Vol. 32, No. 5, 2009, pg. 22-26.
- [2] H. Ching-Jen, T. Amy and Y. Yin-Ho, “Developing an agent-based workflow management system for collaborative product design,” in *Industrial Management & Data Systems*, Vol. 106, No. 5, 2006, pg. 680-699.
- [3] R. Arba, “Collaborative Electronic Marketplace,” in *International Workshop „Collaborative Support Systems in Business and Education”*, Cluj-Napoca, October 2005, pg. 11.
- [4] O. Dobrican, “An Example of Collaborative System,” in *International Workshop „Collaborative Support Systems in Business and Education”*, Cluj-Napoca, October 2005, pg. 48.
- [5] D. Mican, „Collaborative System in Handling Freelancer IT Projects,” in *International Workshop „Collaborative Support Systems in Business and Education”*, Cluj-Napoca, October 2005, pg. 196.
- [6] M. Muntean, “Knowledge Management in Collaborative Environments,” in *The 2nd International Conference on Economics an Management of Networks*, Corvinus University of Budapest, 2005.

[7] T. Daradoumis, F. Khafa and J.M. Marques, "A methodological framework for project-based collaborative learning in a networked environment, in *Int. J. Cont. Engineering Education and Lifelong Learning*, Vol. 12, No. 5/6, 2002.

Authors



Ion IVAN has graduated the Faculty of Economic Computation and Economic Cybernetics in 1970, he holds a PhD diploma in Economics from 1978 and he had gone through all didactic positions since 1970 when he joined the staff of the Bucharest Academy of Economic Studies, teaching assistant in 1970, senior lecturer in 1978, assistant professor in 1991 and full professor in 1993. Currently he is full Professor of Economic Informatics within the Department of Economic Informatics at Faculty of Cybernetics, Statistics and Economic Informatics from the Academy of Economic Studies. He is the author of more than 25 books and over 75 journal articles in the field of software quality management, software metrics and informatics audit.



Mihai DOINEA received a PhD scholarship from the Academy of Economic Studies, Bucharest, Romania in Economic Informatics at the UvA Research Center. He has a master diploma in Informatics Security (2006). He is also a lecturer assistant and he teaches data structures and advanced programming languages at the Academy of Economic Studies. He published more than 20 articles in collaboration or as single author and co-published two books in his area of interest. His research interests are given as follows: informatics security, distributed applications, optimization criteria, databases, artificial intelligence, information management, security policies, mobile devices, networking and wireless communication.