E-Business Security Architectures

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

By default the Internet is an open high risk environment and also the main place where the e-business is growing. As result of this fact, the paper aims to highlight the security aspects that relate to distributed applications [3], with reference to the concept of e-business. In this direction will analyze the quality characteristics, considered to be important by the author. Based on these and on existing e-business architectures will be presented a particularly diagram which will reflect a new approach to the concept of future e-business. The development of the new architecture will have its stands based on technologies that are used to build the applications of tomorrow.
Keywords: *e-business, distributed applications, security, architecture, technology.*

1 Introduction

The Internet in its early stage of development it was intended to help change data, communicate with others very easily and rapidly and to ensure a high degree of effectiveness in working with the new generation of computers that have been in an explosive growth since the early 1990s. Afterwards the Internet was slowly driven to his new age where the basic concept of it was and is commerce. E-commerce is an important part of which the e-business concept is made of. E-commerce represents a new way of making business using the facilities offered by the technologies that are emerging each and every day on the market. The important aspects that characterize e-commerce are:

- large commercial space;
- numerous clients;
- easiness in development;
- easy access on technologies;
- virtual currency;
- transaction speed.

We can assume that e-commerce is a particularly way of e-business. Due to the fact that technologies are rapidly gaining in complexity and number of users that are connected to the network is almost in an exponential growth, the e-business concept has turned him into a wide range of e-things classified in different areas, such as:

- e-commerce;
- e-banking;
- e-learning;
- e-auctions;
- e-government.

As the time passes and knowledge-based society is evolving, ordinary organizations existence is seriously threatened. The only way through which organizations will survive is to redefine them, accepting a reengineering process that will transform them into knowledge-based organizations. At its beginning, the revolution of knowledge had many reasons of technique and technological, human and managerial nature.

Concerning the technique and technological reasons, one can say that the great progress of IT&C field, information processes that are now every day present in our life, communication processes which have reduced the distances between organizations, the atom processes that led to the discovery of new intelligent materials, living cell processes and others discoveries in this area have had a contribution to the forthcoming knowledge revolution.

In knowledge-based society organizations have changed their perspectives and business concept is viewed more through the eyes of customers, partners, so called stakeholders. Knowledge-based organizations is called an organization which based on an economic, ecologic and social balanced approach can exploit knowledge and resources aiming to generate on long term multidimensional effi-

ciency and performance validated by market and recognized by society. An organization who wants to approach to this definition will not have to change very much the organizational and methodological system but will have to work around on the informational system to make it fully automated, more organized and information flow more rigorous defined, not accepting exceptions, those better be treated as parallel informational flows. The decisional system will react more quickly due to the changes to which the informational system has been submitted. In this new approach, decisional system is based on strategic knowledge, data mined from database deposits with tools like online analytical processing, OLAP, that offers competitive advantages to the organization. The strategic knowledge is:

- know-what;
- know-why;
- know-how;
- know-who.

Analyzing the system, e-business turns to be composed of the following components:

- stakeholders component, part of the customer relationship management;
- administrative component, part of the enterprise resource planning;
- informational component, part of the document management system;
- transaction processing used by others components to interact.

How the whole concept of e-business is based on software applications which runs large amount of data on the network stored in databases or data warehouses, vulnerability is its most undeniable threat, which, untreated, in time can lower the sustainability of an organization.

2. Distributed application security

Distributed applications tend to become a widespread factor for the e-business systems in which concept they are incorporated because they increase the efficiency, scalability and reliability. In our days we see more and more organizations that embrace distributed system, with applications that run from multiple locations, databases spread into many places based on the particular needs of each and every organization.

As a result of this decentralization, the needs of network infrastructure are increasing and so are the threats to those systems that send large amount of data through the network, making them more vulnerable to the malicious users who search to intercept or modify network traffic. Common distributed applications architectures are:

- client – server architecture in which a client sends its requests to a server where a the application is executed and then send back a response to the client, figure 1;

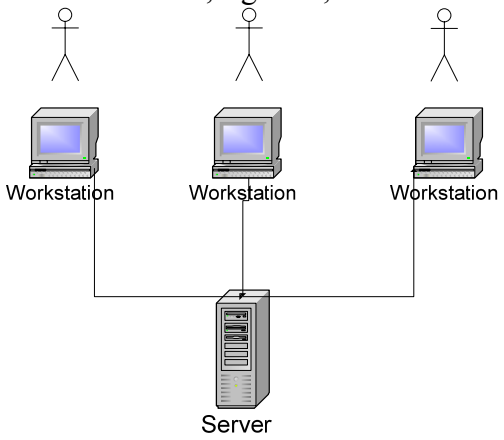

Fig. 1. Client – Server architecture

- peer-to-peer architecture; has no server and each client connects to others through specialized applications for sharing information, figure 2;

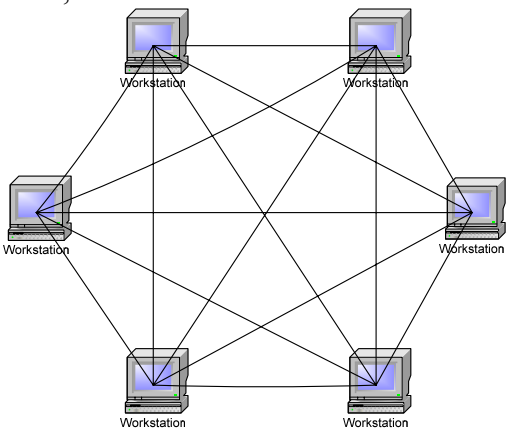

Fig. 2. Peer-to-Peer architecture

- n-tiers architecture are used to separate different levels of application; most common, the 3-tier architecture separates the presentation level from application level and from da-

ta level; all the 3 level can be also divided into other levels, figure 3;

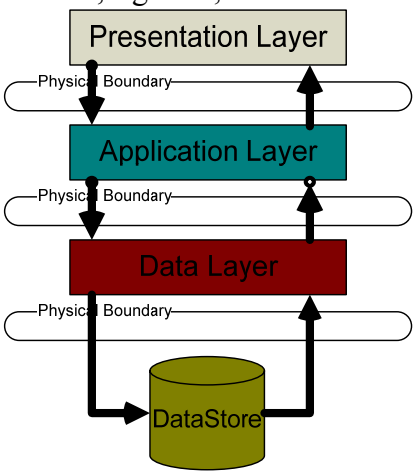

Fig. 3. 3-tier architecture

• DCE architecture used for developing software operating across heterogeneous platforms, figure 4;

Because this architecture presents a high degree of risk the security should be considered a fundamental aspect for the wellbeing of the e-business systems.

The main aspects of distributed applications security are embedded into the following layers:

• administration management through which can be avoided many of unwanted attacks, based on a rigorous authentication process which is the first wall who stands in front of attackers;

• networking infrastructure through which organization changes information;

• database regulations and privileges through which the access to data is controlled;

• organization's access policy to physical equipments;

• software development in the e-business systems that can control any malpractice.

Management issues relate to both the processes of authentication, as well as a permanent surveillance of bugs reported, checking daily logs of applications running on the system.

Authentication is the process that grant users read, write or execute rights to the distributed applications resources. Authentication deals with methods and techniques such as access rights based on username and password, biometric systems, mutual validation of identity, digital certificates rights, multifactor methods of validating identity, CHAP authentication defined in RFC 1994, tokens access, as well as Kerberos methods.

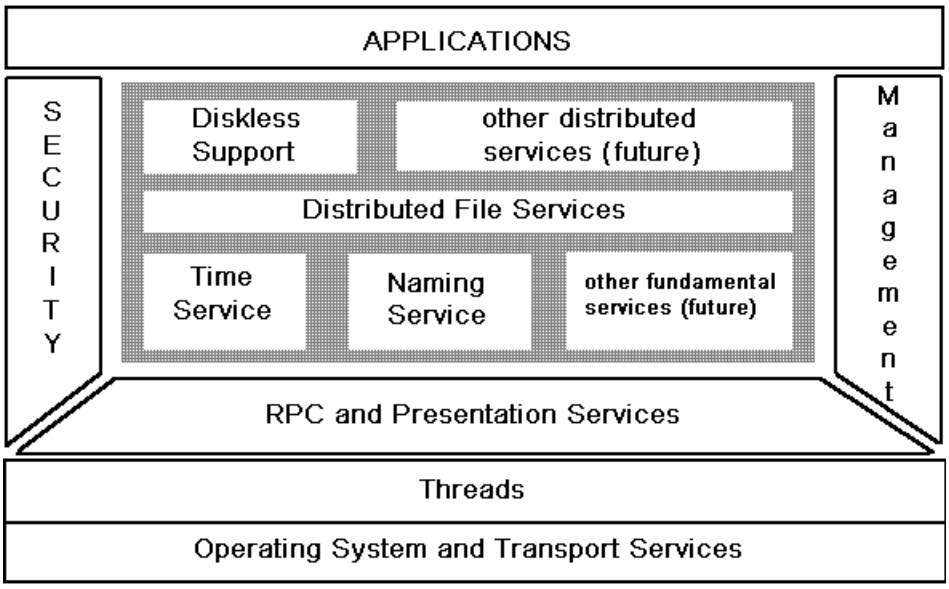

Fig. 4. DCE architecture [5]

Quality characteristics of an authentication process rely heavily on the passwords that are used, which must comply with several restrictions:

• must not contain only alphabetic characters and numbers, but also non-alphabetic as well,

uppercase and lowercase;
- must not be based on a vocabulary to prevent vocabulary attacks;
- must have a sufficient length to prevent brute force attacks;
- account must be blocked after several failed login attempts;
- must be changed on regular basis;
- must not be transmitted over the network in clear text, always encrypted;
- must be unique at least 10 times in a row;
- must not be kept written;
- must only be known by responsible personnel.

On e-business systems, applications that run should be regularly updated, security release patches and updates applied, antivirus programs run frequently. Organizations running e-business systems must have a backup policy in case of disaster in the sense of uncontrolled situations, which are tested and updated periodically.

Communication network security is another important aspect that should matter, as most threats come from outside of the organization, through communication channels. In [2] are presented many methods for preventing any unwanted interception of traffic on the network, mentioning data encryption using symmetric algorithms like DES, RC2, RC4 or asymmetric like RSA. For additional protection, at application layer, can be implemented a firewall to filter any connection unknown to or from the computer. Currently, the best practices for encryption, is a 128 bit SSL encryption having a key with a minimum length of 1024 bits. Another way for communicating properly is by using a virtual private network, VPN, software, which handles all the needs of security in our place.

Database level should be protected by an efficient administration management based on access rights and privileges using as well routers and firewalls. For more protection, data can be kept in a cryptic form, but this, will lower the response time to queries. All sensitive data must be kept on computers that have no access to the internet and none of them must be stored in cache or logs.

Access to equipment must be limited by restricted area and only qualified personnel should manage them. Areas in which sensitive computers are stored must be properly equipped with additional power sources in case of power failures.

Developing software for e-business systems is a huge risk that an organization assumes if any regulations of software development are omitted. There is a large list of best practices in software development from which we'll mention just a few:
- all source code must be reviewed by multiple qualified developers;
- all exceptions must be treated to not reveal sensitive information to users;
- all input data must be validated by several criteria such as length, type or range;
- avoid use of relative paths unless it is necessary;
- source code must not be revealed to anyone, except proper developers;
- executable code must be proper tested, before give it for utilization;
- audit procedures must be passed, for systems to enter into production.

Distributed application development and network communication are the main issues to be considered when running an e-business system.

3. E-Business systems security characteristics

The fast forwardness of today's technology has made users unconscious of vulnerabilities that software may have, leading to a series of security breaches. It is unwanted that users have no idea of what happens behind. On systems that process large amounts of information, such as e-business systems, this can't happen, because vitals information is processed and any untreated vulnerability can be easily exploited.

If we conclude that any untreated vulnerability in an e-business system is a possible loss of vital information, we can say that reliability, non-repudiation, legitimate use, integrity and confidentiality should be the characteristics that an e-business system should have.

An organization that runs an e-business system has to be able for assuring these charac-

teristics otherwise massive losses can be recorded. For this, organizations must:

- keep its systems and services up and running 24 hours a day, 7 days a week, excepting periods when backups or updates are running;
- be able to verify each connection made to the system, identifying users, otherwise rejecting connection;
- assure that each action made in the system is conform with the privileges that the user is having;
- provide trustful information sending to all its stakeholders;
- protect sensitive information through means of cryptography;
- keep logs of every transaction made on the system.

Seeing that were happened and providing the characteristics mentioned above, organizations can perform their tasks without concerning too much for the health of their e-business systems.

Reliability is the capacity of an e-business system to stand up and running every time when needed, meaning that all his services, databases and other resources to be at any user disposal if he is qualified to access them. Reliability is the characteristic that could harm the most in case of its inexistence.

Denial of Service, DoS attack is the main issue that must be treated by any organization that has an e-business system. Many companies have suffered a lot because of an incorrect approach concerning DoS attacks. DoS attacks, as presented in [1], represent the systems inability to respond to users requests because they are blocked by others fictive callers. Any vulnerability that can be exploited by DoS or others attacks that affect reliability like *ping of death, POD* – sending packages larger than 65535 bytes, largest size that can be processed, will generate a buffer overflow error which will lead to a system crash, must be calculated and the risk that it carries must be evaluated.

The following formula could be used for determining the level of vulnerability in an e-business system, *EVL*:

$$EVL = \sum_{i=1}^{n} \frac{p_i f_i}{n}, i = \overline{1,n}$$

$$\text{and } \sum_{i=1}^{N} p_i = 1;$$

where:

p_i – importance coefficient of type *i* vulnerabilities;

f_i – frequency of type *i* vulnerability events;

n – number of executions;

N – number of vulnerabilities.

The ability to face someone's action, with evidence that he did it is called non-repudiation. This characteristic, in an e-business system where lots of transactions are made, is essential. Both parties who participate to a transaction must know the identity of each other and must be capable to prove who has signed it in case of a dispute in a court of law.

Legitimate-use represents the capability of a e-business system to conclude on the following aspects: identification, authentication and authorization. When a user tries to connect to an e-business system, it must identify him, based on the information provided, authentication is the answer afterwards to every user who has passed this stage, a list of privileges are attached, forming the authorization aspect.

Integrity reflects the accuracy and completeness of information that has arrived to recipient same as, when it has gone from deliverer, in his passing through many secure and unsecured networks. There are cases when the integrity is not affected by occurring attacks, as in the case of an eavesdropping or sniffing attack. When the information integrity is affected wanted or unwanted, it is not useful anymore so, this characteristic should be satisfied by an e-business system.

Confidentiality represents the aspect that makes information safety from unwanted viewers. This was not an internet generated issue but came from one of the primarily human characteristics, mistrust. Information processed in e-business systems must only be visualized by persons authorized to do so. This restriction for other authenticated or anonymous users who do not have privileges

to view the information is possible through the use of authentication methods, but for malicious users who use other methods of capturing data traffic, providing this feature is possible by using data encryption.
Scalability is also an important characteristic depending on distributed applications, which are incorporated into the e-business systems. This aspect provides easiness in adding more and more services without lots of changes to the main system. Scalability is necessary because there's no organization that has started from upper levels, but has grown slightly as time passed.
In an e-business system, all characteristics should be treated carefully and no compromise should be taken, since the organization's profit will be affected. And how in a capitalist economy, all that matters is profit, then none should risk the chance, by not doing so.

4. e-Business security architecture - EBSA

E-Business models have become, due to competitiveness and new technologies that have emerged, more complex and more dependent on the IT&C technology. An e-business system is formed by several components that can't run separately and all have a unique goal, realizing the bound between the production process which includes suppliers, production factors, technologies, and the distribution process including customers, products and so on. The difference between income and production costs represents organization's profit.
E-Business can be defined as a business which relies on two concepts: reengineering and integration, concepts that offers major advantages comparing with traditional businesses, such as:

- effectiveness, reflected by the ability to adapt quickly to market changes;
- prompt answers to customer needs;
- efficiency by reduced production costs;
- dynamics, characterized by the ability of e-business concept to reinvent itself, based on the changing needs.

In a time when lots of digital services and products are available to users the e-business brings them closer to the final consumer. But this benefit has its drawbacks. One and too serious it's the security aspects of the e-business systems, precisely, the security of its main components. Figure 5 presents a particularly approach to e-business concept in terms of security: how these main components presented interact and the main frame in which they change information.

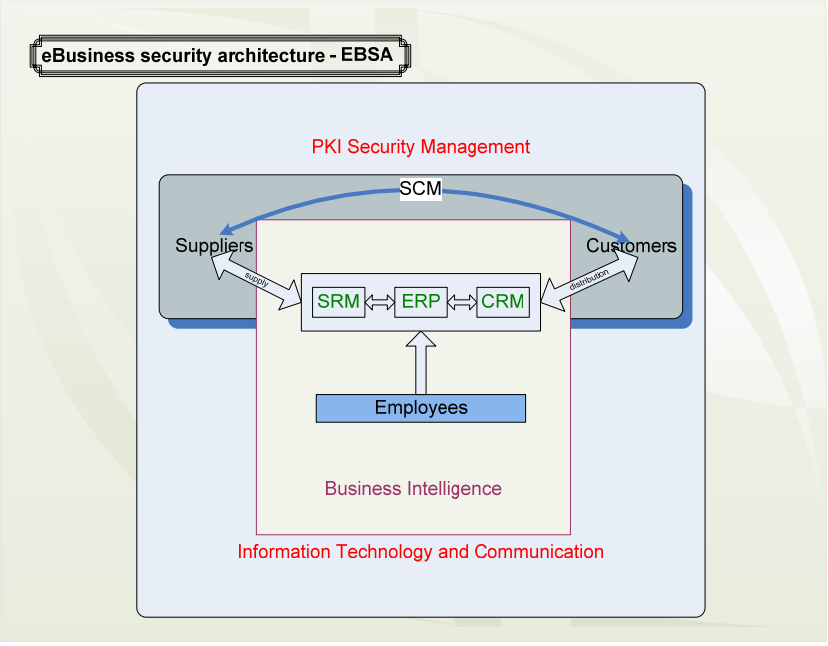

Fig. 5. EBSA, e-Business security architecture

The architecture contains components that can not be omitted, components that interact for assuring the process called as *SCM*, Supply Chain Management. In the context of IT&C, where e-business systems change lots of information, must be implemented a way of securing the integrity, authenticity and reliability of all critical transactions such as financial ones, personal information transactions, decisional strategic transactions based on the OLAP systems. All the strategic decisions are have their fundamentals in knowledge and information stocked in database, data warehouse systems which go us back to the information's security. Data storage security, as presented in [4], is vital for an e-business system for which, mechanisms as LBAC where created for assuring the level of protection which must be applied to every data category. LBAC, which comes from the Label Based Access Control, group information into categories according to the sensitive characteristic, assigning labels. Based on these labels access is restricted if privileges are not met to satisfy the sensitiveness of information.

Transactions found on each and every component can be secured using encryption techniques, can therefore cross unsecure networks without the risk of compromising information on its quality characteristics. The components on which the presented architecture is based on are:

- applications for Customer Relationship Management, *CRM*, used for interacting between various departments such as sales, marketing and client services; the main aspects of these applications is client orientation, trying to provide the best services to customers and collecting feed-back for interested departments;
- *ERP* applications, Enterprise Resource Planning, are focused on planning based on forecasting, procurement management, materials, inventory, accounting information, such as receivables and payments; *ERP* applications make the leap from the stock based production to requests based production;
- *SCM,* Supply Chain Management helps to optimize production process, managing stocks and decreasing the expectation time of customers by fasting up the delivery time; at their full efficiency *SCM* applications can break the disadvantages generated by logistics;
- Business Intelligence, *BI* is the picture frame in which are managed the applications described above; it refers to knowledge, skills, technologies, services, risks, security issues, applications and more others that are used for stepping the traditional business into a new era of making business.

Those concepts are relying on the efficiency of the security systems which are incorporated into the functional ones. Security can be very well achieved by implementing a *PKI,* public key infrastructure, like the one presented in figure 6.

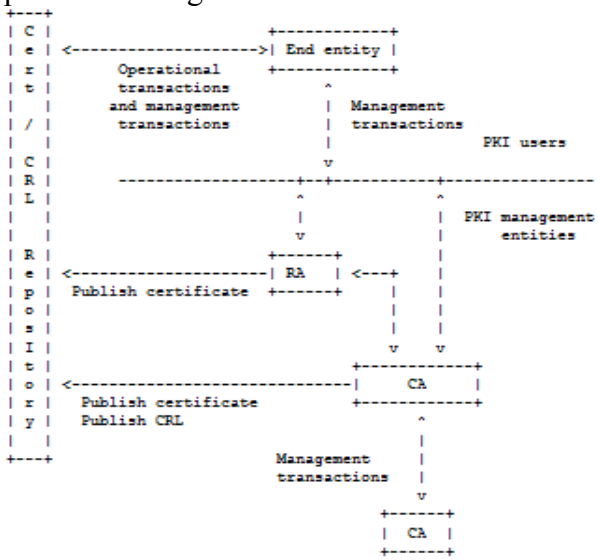

Fig. 6. Internet X.509 Public Key Infrastructure, [6]

The components presented are:

- end entity – user of PKI certificates or/and a end user system that is the subject of a certificate;
- CA – certification authority; the one who issue a certificates for end entities;
- RA – registration authority;
- repository – a collection that includes certificates and CRLs for distributing to the end entities.

The public key infrastructure goals are to meet the needs of security at each level of e-

business systems assuring the identification, authentication and authorization functions.
Certificates registered and emitted by a certification authority are more reliable then the systems based on username and password having information encrypted with the public key of the owner inside them. Using public key infrastructure does not imply restrictions for the systems on which operates.

5. E-Business technologies

For that e-business system to have high level of automation without needing large number of personnel, advanced technologies must be used for developing system functions, technologies able to develop complex and reliable applications whose execution threads are running on multiple locations. Object oriented programming must be implemented by these technologies for allowing the concepts of encapsulation, abstraction and polymorphism. These options are embedded in .NET platform, Java RMI, remote method invocation, which can create reliable, complex distributed applications.
Microsoft has released in late 2000 the first version of .NET Framework 1.0 able to develop distributed applications with minimum support. Using the capabilities offered by the Common Language Runtime – CLR, the platform had put all .NET programs to run under the same surveillance of virtual machine. Common language runtime offers memory management, security and exception handling uniting all .NET languages under the same MSIL – Microsoft Intermediate Language. Lately versions as .Net Framework 3.5 or even 4.0 announced recently include lots of components like:

- LINQ – Language Integrated Query, a native language syntax for queries that runs over C#, Visual Basic and XML;
- Windows Presentation Foundation, WPF, coded as *Avalon* represents a new set of API based on XML and vector graphics using the 3D hardware capabilities of the computer;
- Windows Communication Foundation, WCF, called as well *Indigo* specially designed for e-business applications allowing them to interoperate locally or remotely;
- Windows Workflow Foundation, WF is very useful for developing automation tasks using workflow events for production process, customers support and other e-business functions;
- Windows CardSpace, a software component that allows users to securely store their authentication information.

For developing distributed application .NET Remoting is one of the most important tool of the platform. The disadvantage is that all systems must have the .NET platform installed too. In .Net Remoting libraries are implemented 2 types of classes that can be used for developing distributed applications:

- serializable classes that can be used for sending objects as streams through the network; for this, developers are using 3 types of formatters to proceed to the process of serialization and deserialization: binary, soap and abstract formatters;
- marshal classes that offer the possibility for allocating unmanaged memory, copying unmanaged memory blocks as well as converting managed to unmanaged types.

Sun Microsystems has called his object orientated language JAVA, developing a platform and a java virtual machine just like the .NET Framework, having a set of libraries, Java API compared with the BCL, *Based Class Library*, of the .NET Framework. Java uses remote classes to implement the communication processes for the distributed applications. Using RMI, Remote Method Invocation, objects that run on a Java VM can invoke methods or properties from other objects that run in different Java VM.

6. Conclusions

E-Business systems have become indispensable for most of the large organizations because of the huge development of today's technology and the huge number of competitors that used them. The development from the early 1990 until now had shown a great potential of the technologies which will lead to a world where e-business will easily be implemented at large scale even in small organizations. Concepts like SMS Marketing had emerged in the last few years revealing

the path which e-business will step. Organizations tend to automate most of their process to reduce the production costs. E-Business systems development cause security to be more effective, therefore, as e-business systems will gain new features and the IT&C will be used by more and more users, the security will need to keep the line straight, assuring those information characteristics that always will be necessary.

E-Business systems are dependent on all the application from which they are formed of. Any vulnerability found at these levels is affecting the main system causing possible unavailability which is equivalent to huge costs for organization.

Under the expression *"what today amazes us tomorrow may seem commonplace"* e-business systems will develop and more security technologies will rise to stand up the threats that come from the World Wide Web.

The paper was financed from European Structural Funds, project no. 7832, "PhD and doctoral in the triangle Education-Research-Innovation, DOC-ECI" (cercetare finanțată din Fondurile Structurale Europene, proiect nr. 7832, "Doctorat şi doctoranzi în hiul Educație-Cercetare-Inovare, DOC-ECI").

References

[1] I. Ivan and C. Toma. *Informatics Security Handbook*, ASE Printing House, Bucharest, 2006

[2] V. V. Patriciu and I. Bica. *Electronic signatures and Informatics Security*, ALL Printing House, Bucharest, 2006

[3]C. Toma. *Security in software distributed platforms*, ASE Printing House ASE, Bucharest, 2008

[4]M. A. Davidson, "Security for e-Business," *Information Security Technical Report*, vol. 6, no. 2, pp. 80-94

[5]http://www.fas.org/irp/program/core/dodiis/sec2-6.html

[6] http://www.ietf.org/rfc/rfc2459.txt

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.