The confidentiality – integrity – accessibility triad into the mobile Commerce and business

Popescul, Daniela

Alexandru Ioan Cuza University

20 June 2007

Popescul, D., *The Confidentiality – Integrity – Accessibility Triad into the Mobile Commerce and Business*, în **Information Management in the Networked Economy. Issues & Solutions, The Proceedings of The 8th IBIMA Conference**, Dublin, Ireland, 2007, ISBN:0-9753393-7-0, pp. 527 – 533

The Confidentiality – Integrity – Accessibility Triad into the Mobile Commerce and Business

Daniela Popescul, Business Information Systems Dept., Faculty of Economics and Business Administration, "Alexandru Ioan Cuza" University, Iaşi, Romania, rdaniela@uaic.ro

Abstract

The necessity of considering the three main faces of informational security mentioned in the title of the paper derives from the accumulation of the importance of the data circulating in the mobile environment for organizations, with the existence of numerous dangers and threats that target these data. After a general presentation of the dangers that can affect mobile business and commerce, structured on three main categories, the article surveys the B2C mobile commerce services and the main types of mobile applications used within organizations, re-dealing with the need for confidentiality, integrity and accessibility of the information turned mobile.

The paper is mainly addressed to the managers interested in the use of mobile devices in the activity of the organizations they lead, warning them about the sensitive points of the mobile activities, with the dangers associated with them and suggesting them that the traditional security mechanisms have to be expanded and sometimes improved in mobile services.

Key words: *mobile commerce, mobile commerce security, mobile Internet, mobile business*

1. Introduction

The necessity of ensuring the security of mobile commerce and business is transparent even from their definitions. Two big names from the literature regarding electronic business, Ravi Kalakota and Marcia Robinson, insist on the fact that the mobile commerce transactions are administered *in motion* and that they are, especially, *buying* and *payment* transactions.[1] Considering the fact that the exchanges have as object products, services and money, the need for security derives from their nature and needs no further justification. The ADCOS software company defines mobile commerce *as the mobile consumer's possibility to obtain goods and services* ***in a safe mode***, *through the wireless technology*. [2] The security requirements become even more stringent in the case of mobile businesses, broadly defined as *a new form of use of the informational and communications technologies in view of integrating the value chains and the business processes*, a form which facilitates the communication and coordination within the organization, as well, overall, its management.[3] The particular characteristics of the mobile businesses are *interactivity, the almost permanent availability and personalization*. In order for them to be achieved, the security of the data involved is a sine qua non condition.

The problem of the security of data in the mobile environment is treated, either tangentially, or in deeper ways, in different materials. Paul May treats various problems regarding the wireless standards and the use of the PKI infrastructure.[4] Technical aspects and comparisons between the security needs in the fixed internet and the mobile one appear in Norman Sadeh.[5] In articles from the press in the field there are concerns being formulated regarding the security of mobile payment transactions [6][7][8][9][10] or of the personal information stored on portable devices. [11]

Next, we will try to structure the dangers that hang over the use of mobile devices in business, depending on their nature. Also, in a new approach, we will treat the dangers specific for certain areas of mobile commerce and business, emphasizing the importance of the confidentiality – integrity – accessibility triad for each of them.

2. General vulnerabilities and threats in mobile environment

To shop online using a mobile device, consumers need to feel the same sense of security as when they shop in the physical world. The issues of confidentiality, privacy, integrity and accessibility of data, information and transactions being exchanged from one point of the wireless network to another could be seen as a key barrier to transforming mobile solutions into reality.

In this spirit, we present a set of threats and vulnerabilities which appears in mobile commerce and mobile business, categorized in:

- Devices vulnerabilities;
- Network (technological) vulnerabilities;
- Human threats.

The risk of *loss, theft or damage* is very likely in case of mobile **devices**, because of their portability. By stealing a mobile device, a thief can use it in mobile transaction, in the name of real owner. When the mobile device has sensitive information on it, important security issues appear. In short, device ownership is the main issue: although anyone can pick up the device, only its owner must be allowed to carry out transactions involving personal data. The best solution for that situation is to never store any data in the device, but it is equivalent to a "Faraday cage", with its advantages and disadvantages. There are companies which have developed programs that lock down the device, or encrypt the data on the device. These approaches bring a serious problem

with them: the user has to log on to the mobile device over and over again, with every transaction he wants to initiate. This seems like another kind of Faraday Cage. A better approach would be biometrics. A handheld that could read a thumbprint to authenticate the user would make everything easier.

The mobile devices could also be cloned. *Cloning* is about copying the identity of one mobile phone to another, for the purpose of making fraudulent or anonymous telephone calls. [12] In our case, by cloning, an attacker could buy goods and services in the name of real users, which will pay them. Cloning involves modifying or replacing the EPROM in the phone with a new chip which allows the attacker to configure an ESN (Electronic Serial Number) via software. The MIN (Mobile Identification Number) would also be changed. ESN/MIN pairs could be discovered in several ways:

- Sniffing the cellular networks;
- Trashing cellular networks or cellular resellers;
- Hacking cellular networks or cellular resellers.

Newer phones are difficult to clone. It is still possible to clone a GSM phone, but the process is difficult, needing a serious research. In most cases, it doesn't worth the effort.

Mobile malware (viruses, worms and Trojan Horses) are only one type of **threats in mobile networks**. To date, all mobile viruses are relying totally on user action. A recipient has to accept and download an application in order for the "attached" malware to be launched. On the other side, in spite of great media hype, existing malicious software is composed rather of proof-of-concept codes than real threats. No virus, worm or Trojan Horse has yet broken the security protection of mobile phones, without the accept of user. The reason for that is the wide array of different phone models, network technologies and embedded operating systems. Mobile operating systems and devices manufacturers and also mobile communications operators have, at this moment, a tighter control over their environment. More than that, there isn't (yet) a big mass of people using a certain technology – when this would exist, the "specific" viruses will appear for sure. This affirmation is confirmed by prevalence of viruses' attacks on the GSM Nokia phones with Symbian operating system, which are the most used in European area. In future, in some opinions, a nightmare will begin. "The virus would delete the contents of your phone, or start calling a toll number on its own from the phone or recording every single one of your conversations and sending the recorded conversation somewhere" (Mikko Hypponen, director of anti-virus research at F-Secure Corp., a Finnish security firm).[13]

There are also other *various attacks, permitted by technology*. For example, the best-known Bluetooth vulnerabilities allow illegal access to information stored on mobile phones. Some *blue*-prefix attacks are *bluejacking* (spamming nearby mobile phone users with unsolicited messages), *bluesnarfing* (stealing the contact information found on vulnerable devices), *bluebugging* (accessing mobile phone commands without notifying or alerting the phone's user; the hacker can initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet).[14] In all this attacks, the hacker must be within a 10 meter range of the phone. Less original and pretty harmless because of the short range coverage of technology, *Denial-of-Service* is also possible with Bluetooth. The mobile DoS attack consists of constant request for response from a hacker's Bluetooth enabled computer to another Bluetooth enabled mobile device. Beyond annoyance, such an attack causes some temporary battery degradation in the receiving mobile device. Data are not affected; they can not be used or stolen by the hacker. Leaving Bluetooth alone, we will observe that security is not built in GPRS, EDGE, 1xRTT, EvDO, or in other mobile protocol. In this situation, encryption must happen in the device, before the data are even sent.

The **human threats** are referring *to hackers' attacks* (which are more or less presented previously), but also to the *employees actions* (which are, in most of the cases, errors caused through ignorance). An organization could adopt a multitude of approaches. For example, by spending some money, it could provide employees with devices and the software application able to ensure that they are secure. This is the best solution, there are some projects in this sense, but it is not happening on a large scale. The real situation is worse: people use their own devices to access e-mail and calendar information, but also financial and organizational data. As a result, sensitive information ends up roaming around freely. The organizational security policies, where exists, are not very efficient: a company could not recommend what to do to an employee who has spent a lot of money on its mobile device.

3. Aspects regarding the security of information in B2C mobile commerce

Next, we will approach the confidentiality, integrity and accessibility of data within the main services of mobile commerce.

Mobile commerce is completely different from the retail sale of goods on the traditional Internet. Only part of the goods that are the object of traditional electronic commerce can be sold *exclusively* through the mobile networks and devices. They are mainly digital products. For the other goods, more "palpable", the mobile retailers are compelled to go into partnerships with environments such as the written press, radio, television, in order to provide in comfortable way information about the

characteristics of the products. Even in the case of some functional partnerships, few goods and services are the object of mobile commerce.

One of the first services tested on the mobile devices capable to connect to the Internet is **ticket reservation and purchasing** for different events (theatre, film, concerts) or for the transportation means (auto, train, plane).

In the situation when in the transaction, tickets for certain events are involved, the associated risk is low, because the only possible loss is that of the value of the ticket. For the purchasing of a ticket the disclosing of personal information is not necessary and, in most cases, nor is that of the financial information. The simplest (and safest) way of effective delivery of the tickets is reserving them through the mobile phone and then paying the equivalent value and receiving them at the ticket desk, after the communication (in person or through a transmission technology such as Bluetooth) of a code received when making the reservation. More technological solutions also offer the possibility of paying directly, when ordering, by charging it on the mobile phone bill or through a mobile banking application. It is obvious the fact that the risks increase gradually in the case of the three solutions presented. In our opinion, in principle, confidentiality is not a major requirement, especially if the ticket sale/purchase is done under the protection of anonymity.

We do appreciate though that special attention has to be granted to avoiding the occurrence of errors in the mobile ticket reservation system, especially in airports. In this sense, the integration of the automatic ticket delivering systems through mobile Internet is an essential condition. Some theaters or cinemas, airports or railroad stations have already implemented applications that allow the purchasing of tickets on the fixed Internet. They are also prepared for the mobile Internet, because their back-end systems connect to the Internet in real time. Problems and concerns appear when the projects have a broad coverage, and the possible losses in the case of bad management are big. In the case of the Simplify the Business project, initiated by *IATA (International Air Transport Association)*[15], who intends, among others, to transform the boarding ticket into a digital bar code, registered as an image type message on the mobile phone and scanned at boarding by a special device, the accuracy of the systems is a mandatory requirement, especially under the conditions of the terrorist threats the airlines are confronted with at the present.

The interception of the image type messages, their counterfeiting etc. makes the integrity of the systems the most important concern of the suppliers of these services. The accessibility, the availability of the tickets in real time is also a mandatory requirement.

The main vulnerability in the case of the commerce with **ring tones, logos, music and games** in the mobile environment consists of the risk of their piracy. There are concerns mainly about the music download in audio form and its free sending, as an MMS message, to friends and acquaintances. A solution would consist of developing a system based on encrypting keys, which would be stocked on the SIM card and on the server and used in order to download, listen and transmit music, videos and games.[16]

The risks afferent to the delivery of **news and information** destined for the possessors of mobile phones depend, firstly, on the importance of that information for their solicitant.

The essential requirement in this case is, with no doubt, the accessibility of information in real time, as is seen in the following examples:

- in the case of news, it is obvious that their availability at the right time is essential, because out-of-date news are not useful to anyone;
- in the case of an application that informs, for example, through SMS, the parents about the school situation of the students, important is the accuracy of the communicated results and the absence of any distortion of these, as well as the information in due time, so that corrective measures can be taken;
- if the results for an admission exam are transmitted, for example, through SMS, it is very important that they are the real ones and that they reach the candidate as soon as possible etc.

For some of this information (grades, exam results, flight schedule etc.), requirements for confidentiality can also come up and, with no doubt, for integrity.

If in the field of **mobile auctions and stock exchange transactions** the main requirement of security is also given by the availability in real time of the data, we can say, without hesitation, that the most vulnerable area of B2C mobile transactions is that of **mobile payments.**

In the case of mobile payments, especially important, besides the money itself, is the financial information regarding the accounts of the users.

Mobile payments have *varied forms of concretization*, presented in the following enumeration. The associated risk levels also vary, in turn:

- The adding of the equivalent value of the purchased goods or services to the mobile phone bill, a method that has the advantage of being familiar to the user. For example, when buying a good through a site and specifying this method of payment by the buyer, the seller gets in touch with the mobile phone operator, who supplements that value on the bill of the user (the *m-pay* service of *Vodafone* works in this way). In this category the payment through SMS with added value is also included. The risks are low, because the payment by billing mechanism is one

tested by the mobile phone operators along their activity;

- The deduction of the mobile payments from the user's credit account; the mobile phone works as a credit card; an alternative of this type of payment is the extraction of the owed sum of money from a separate account of the buyer, dedicated for the mobile payments (the risks are reduced, but the user has the extra care of managing a new bank account). The security of the payments is, in this case, the duty of the banks;
- Payments from virtual accounts or from pre-paid SIM cards – the virtual sums are actually the proof of the previous payment of a certain amount of money to an issuer of such payments solutions. The „charged" sum can be spent through the mobile technologies and, of course, reconstituted through subsequent deposits. The payments from virtual sums are especially used by persons who do not have a bank account (such as children, individuals in isolated areas). Their advantage is the low risk, for all the parts involved in the transaction. The main disadvantage consists of the fact that the blocking of an amount of money in a virtual account does not bring any gain to the user, but rather to the providers of this payment solution; besides, the „depositing" of the sum is an extra step in a transaction where the main advantage should be simplicity;
- Other payment methods: transforming the loyalty points into currency for various acquisitions; pay-as-you-go (used in the case of video games, for example). The risks are also reduced, since it is mainly about micro payments.

The main threat that targets the mobile payments is the **effecting of a fraudulent transaction**. It can be realized through the interception and use by an attacker of the PIN code, of a password, of the MSISDN number and by interposing the attacker in the communication between the possessor of the payment application and the bank and the sending of messages in the name of the real participants to the transaction (mobile spoofing). If the operator of the mobile payment (the bank or the phone operator) leaves the care of the protection through PIN or password to its possessor, the risks increase from well-known reasons: in order to avoid memorizing some difficult PINs and passwords, the individuals associate them with personal data, making them easy to find out. Special attention has to be taken in the case of macro payments, when more powerful authentication procedures of the payer are necessary (PIN, name of the user and password or even authenticity certificates), while in the case of micro payments the authentication can be made only based on the PIN verified by the operator or the bank or it can also be absent.

The identity theft, that is, the interception of personal data of the user of the mobile payment and their use, in a way similar to the traditional internet, to extract money, can be counteracted by using a mobile wallet. Virtual wallets are applications installed on the mobile phone and stocked in a safe environment (a card, a personal computer or a server, usually found at the mobile operator), who contain information about one or several accounts of the user, as well as personal information about him. The stocked data are: the identity of the payer, the authentication data (PIN, password, asymmetrical keys, authenticity certificates) and the payment data (the card account number, the amount stocked on the wallet). The main advantage of the virtual wallet is the quick and safe acceptance of the information needed for closing a payment, without being necessary to fill out forms, an operation which is difficult in the case of mobile terminals. Mobile wallets also ensure the security of the payment: they have passwords similar, but distinct from the PIN number – thus, the loss or theft of the phone is not a problem from the point of view of the security of the "finances" of its possessor. It is estimated that, in the case of the development of mobile payments, virtual wallets will be one of the key technologies in this area.

	Confidentiality	Integrity	Accessibility
Mobile ticketing	◔	◕	●
Ring tones, logos, music, games	○	◔	◔
News, Information	◑	◕	◕
Mobile auctions	◕	●	●
Mobile payments	●	●	●
Mobile positioning	◕	◕	◕

Fig 1. The need for confidentiality, integrity and accessibility in mobile commerce services

The payment through the mobile phone seems safer than providing the details of the credit card to a human operator. Security mechanisms such as digital signature and PKI contribute to the feeling of safety. Still, the computer attackers have easily adapted their methods for the sector of mobile communications. Along with interceptions or mobile viruses, already "in use", there can also emerge dangers such as identity theft (through phishing and phreacking). Moreover, many times, especially for micro payments, the implementation of some supplementary security mechanisms would prove to be too costly.

The confidentiality, integrity and accessibility have to be ensured at the highest standards in the case of mobile payments, as shown in the table 1.

The mobile applications can be expanded with **localization (positioning)** functions. The benefits that these supplementary modules of the mobile

applications bring are convenience, time and money saving, psychological motives such as belonging to a group, image boost, satisfying the curiosity regarding new things. The mobile applications based on locating are of two main types: pull and push. Essential, especially in the case of the push services are security and privacy. In case of security breaches, third parties will be able to track down the position of the individuals and use this information for questionable purposes.

4. Aspects regarding the security of mobile applications within organizations

Next, we will approach the security of the information used in the mobile applications within the organizations, analyzing the subject from a horizontal and, respectively, vertical perspective.

4.1 The horizontal approach of the security of mobile solutions

Mobile solutions for managing the specific tasks by the employees represent a way to solve the administrative tasks at the level of the organization, very useful for the companies who have many employees on the field. The mobile devices equipped with portable printers, bar code readers or electronic signature generating devices allow the solving of all work tasks "on the site", where the employees work. The costs with drawing up documents on paper are reduced, and the employees can take care of many administrative tasks without having to travel to the company office.

At the same time, the employees stock on these supports their personal data and they have access to all the information within the firm that corresponds with their work tasks. Besides the care for ensuring the privacy of the individuals, the persons responsible with the security within the company have to take into account the fact that the security policies used at the level of the organization have to also be respected outside it, by the mobile employees, and the stipulations from the confidentiality and fidelity contracts are not more gentle if the work is not performed between the physical walls of the company.

One of the problems that emerge as a consequence of equipping the employees with mobile terminals is the fading of the border between work and entertainment, as well as the dilution of the concept of "work hours". Through an adequate security policy of the firm, there can be found a balance between the use of the mobile phone for solving the work tasks and using it for personal purposes.

All the big providers of **ERP** offer …mobile modules, able to execute tasks such as:

- the management of orders (filling out an order form, by selecting and visualizing the products from the catalogue, along with their prices);
- the management of clients (creating, updating of records about the clients, sending e-mails, listing the most important clients or the clients depending on certain criteria; information about the product bought, history of previous interventions);
- the management of personal activities;
- the management of the product catalogue;
- the administering of requests from clients, the registering of solicitations and complaints;
- the progress of the service and maintenance activities by the engineers from the client's home or from elsewhere, by extracting the information needed from the back-end system of the firm;
- sending the final reports, tallies, lists with the necessary materials at the end of the work day by the employees on the field;
- the mobile deployment of the procurement activities, through modules such as the mobile purchase basket.

From the enumeration of the tasks above, one can easily notice the fact that the mobile modules of ERP applications send parts of the database of the organization over-the-air, towards their users. The data on the mobile devices has to benefit, in this context, from at least the same level of confidentiality as the data from the "original" database. Their integrity is essential and it must not suffer as a consequence of their transfer between the mobile devices and the fixed database, on the servers of the organization. The security of the application, in this context, is achieved through SSL, the encrypting of the local database (on the mobile device).

A **CRM mobile solution** is a solution that puts the CRM applications at the disposal of all users, who need them, regardless of the place where they are and of the time of the request. By "user" is meant any person involved in the relationship with the clients, from within the organization or outside it. The clients, suppliers, employees and other partners of the organization can use a collaborative CRM solution with the help of the mobile devices, of the Internet applications and of the wireless Web. A CRM application gravitates around a database where the elements that describe the relationships with the consumers are stocked (contact information, history of the transactions with that clients, previous assessments and the personal interests of each client). In this way, the ones who work in sales and service can have a more accurate image on what is best suited for the clients, formulating their offers better and adapting their interventions to the interests of the solicitant. This information, though, is part, in most of the cases, of the area of information especially valuable for the company. Special care has to be given to the collaborative solutions, which allow the sharing of certain information with the business

partners. No matter how close they are to the mother company, the managers have to see if in the partner firm security mechanisms at least as powerful are implemented. The partners also have to have a comparable system of classification of the information, so as to not have problems because of the possible declassifications of the information. The persons responsible for security have to carefully filter the information that will be sent to the partners, so as to not allow them a too intimate closeness with the database and in order to not transform them from friends into enemies.

The same requirements have to also be ensured in the **SCM** (Supply Chain Management) applications, whose purpose is broader than that of CRM. They target the building of a complete cycle of sales, from the contract with the client to the delivery of the product, for the invoicing of the transactions and the finalizing of the sale.

The **remote control of applications and equipments**, in the mobile alternative, is used to reduce the operational costs, to ensure the security and to increase the quality of the repairing and maintenance activities. The devices needed for these applications have to be equipped with GSM, TDMA or CDMA, a battery, an incorporated antenna and a GPS receiver (if the locating of the equipment is necessary).

Table 1: The need for confidentiality, integrity and accessibility in various area of activity

	Confidentiality	Integrity	Accessibility
Constructions	The data accessed do not have a high sensitivity level. It is about the availability of materials and equipment, tallies, orders etc.	Important, but not vital	Important, but not vital
Emergency services and medical assistance	The data used are many times sensitive, being connected mainly to the medical history of the patients.	Vital, literally	Vital, literally
Finance	The information regards the increase of decrease of the stock quota, the reaching of a limit in the bank accounts etc. They are part of the confidential information area.	Important, sometimes vital	Important, sometimes vital
Insurance	The situation of the targeted clients is the main interest of the insurers. It is not information with a high level of confidentiality.	Important, but not vital	Important, but not vital
Logistics and transport	The data accessed from the mobile devices refers to the destination of the delivery, route and other similar data. They are not extremely important.	Important, but not vital	Important, but not vital

The mobile solutions for remote data reading are welcomed in the places where traditional stations, with phone and human operator, can not be installed, or where the installation would be too costly. But if the data that they have to communicate are vital (the discharges of the gas pipes from the field that have reached a below minimum level, for example) advanced solutions for encrypting and sending the data in real time will be more than necessary.

4.2 The vertical approach of the security of mobile applications

The analysis on horizontal levels is not complete if we do not also approach the problem from the point of view of the area of activity for which the mobile solutions are very adequate. It is about areas of activity where there are several mobile employees involved, such as construction, emergency services and medical assistance, the financial field and that of insurances, logistic and transport.

5. Conclusions

As a result of its great expansion, mobile telecommunication has become exposed to information security and safety hazards. The vulnerabilities and attacks are various, caused by technological limits of mobile devices and transmission techniques. But their impact is not very high; they are isolated and, in most of the cases, released under laboratory conditions. Even if the mobile vulnerabilities scene seems to be in its infancy, the importance of security is great in case of mobile commerce, where financial and personal data are involved, and very high in mobile business, which are gravitating around confidential and secret organizational data. The security solutions market responses quickly to the new-founded mobile threats. The "mobile" manufacturers make their devices and their software application better and better. First mobile virus scanners, encryption and VPN products were emerging. This situation takes to a growth of users' trust level, and it's promising

for the mobile commerce and mobile business future.
In this paper, we tried, through a new approach, focused on the analysis of the dangers, vulnerabilities and the importance of data on types of mobile applications and commerce, to bring into attention the necessity to ensure the confidentiality, integrity and accessibility of information in those respective areas. The mentioned triad can prove to be vital in mobile payments, for example, or in services such as those of ensuring the health of the individuals. In the other analyzed areas, either the confidentiality of data can be important, or their integrity, or their accessibility. Knowing what the essential characteristic that they have to pursue in a certain sector is, the managers will know which methods are the most appropriate for the protection of data. In this regard, we appreciate that, starting from the present paper, in the future it would be interesting to approach the appropriate security measures for each type of mobile commerce service individually.

6. Acknowledgement

This paper was published thanks to the funding from **Grant CNCSIS AT 155/2007.**

7. References

[1] Kalakota, R., Robinson, M. *mBusiness (The Race to Mobility),* McGraw Hill, New York, 2001, p. 5

[2] ADCOS software company definition, Retrieved June 15 2005, from: http://www.adcos.ro/v6/index.php?lang=ro&id_page=m-comm_what

[3] Barnes, S. J. *m-Business: The Strategic Implications of Wireless Technologies*, Elsevier Butterworth Heinemann, New York, 2003, p. 2
[4] May, P. *Mobile Commerce (Opportunities, Applications, and Technologies of Wireless Business),* Cambridge University Press, UK, 2001, pp. 227-233

[5] Sadeh, N. *M-Commerce. Technologies, Services, and Business Models*, Wiley Computer Publishing, John Wiley & Sons, Inc., 2002, pp. 131-156

[6] Mallat, N., Rossi, M., Tuunainen, V. K. „Mobile Banking Services", *Communications of the ACM*, May 2004, Volume 47, Number 5

[7] Butiri, A., Niţchi, Ş. "Mobile Banking", *The Proceedings of the International Symposium Specialization, Development and Integration*, Cluj-Napoca, Romania, 14-15 November 2003, S.C. Roprint S.R.L., Cluj Napoca

[8] Caprita, D. A. „Mobile Commerce", „*Information & Knowledge Age" (The Proceedings of Seventh International Conference on Informatics in Economy)*, Ed. Economică, Inforec Printing House, Bucureşti, 2005

[9] Hinds, D. "Micropayments: A Technology with a Promising but Uncertain Future", *Communications of the ACM*, May 2004, Volume 47, Number 5, p. 44

[10] Kharif, O. "Cell Phones vs. Credit Cards: The Battle Begins", *Business Week*, June 28 2005

[11] Czerwinski, M., Gage, D. W., Gemmel, J., Marshall, C. C., Perez-Quinonesis, M. A., Skeels, M., Catarci, T. „Digital Memories in an Era of Ubiquitos Computing and Abundant Storage", *Communications of the ACM*, January 2006, Vol. 49, No. 1, pp. 45-50

[12] Oprea, D. *Protecţia şi securitatea sistemelor informaţionale (Information Systems Protection and Security),* Polirom Publishing House, Iaşi, România, 2003, p. 201

[13]***, Skulls Mobile Phone Malware On the Loose, Retrieved August 2005, from: http://www.wormblog.com/2004/11/skulls_mobile_p.html

[14] www.bluetooth.com/help/security.asp
[15]*** "Change is in the Air", *The Economist Technology Quarterly*, March 12th 2005, pp. 16 – 18

[16]Balaban, D. In a Multimedia World ... Whither the SIM Card?*, Card Technology*, February 2004, p. 38

[17]Paavilainen, J. *Mobile Business Strategies (Understanding the Technologies & Opportunities),* Wireless Press (Addison Wesley & IT Press), London, 2001

[18] Rusu, D., The (In)security of Mobile Commerce, *Proceedings of InfoBUSINESS'2005 - „Innovative Applications of Information Technologies in Business and Management",* October 14-15, 2005, Iaşi, România, PIM Publishing House, Iaşi, 2005

[19]Vos, I., De Klein, P. *The Essential Guide to Mobile Business*, Upper Saddle River, Prentice Hall, New Jersey, 2002