Information Security for Sustainable Development

Halit Vural
International Burch University
Faculty of Engineering and Information Technologies
Sarajevo, Bosnia and Herzegovina
hvural@ibu.edu.ba

Nejdet Dogru
International Burch University
Faculty of Engineering and Information Technologies
Sarajevo, Bosnia and Herzegovina
ndogru@ibu.edu.ba

Abdulhamit Subasi
International University of Sarajevo
Sarajevo, Bosnia and Herzegovina
asubasi@ius.edu.ba

Abstract: With the advent of electronic commerce (e-commerce), business became dependent on information systems in a new manner. Consequently information security turned out to be more and more important for data-protection. In opposed to previous systems, the changing requirements for security must be solely filled by new policies and risk analysis. Security requirements can be defined with the help of investigations in the business environment. Mobile commerce (m-commerce) is a rising discipline which includes applications, mobile devices and wireless networks. Besides the majority of existing e-commerce applications can be adapted to run in a wireless environment. M-commerce also involves many more new applications such as, mobile financial services, user and location specific mobile advertising, mobile inventory management. Therefore, most of the m-commerce research should focus on applications, and security issues. To supply these demands, we need to understand the necessary security requirements for every kind of implementation. The aim of this work is to describe an approach for the importance of the information security for sustainable development.

Keywords: Information Security, e-commerce, m-commerce, e-government, wireless networks, Sustainable Development, survivability.

1. Introduction

In recent years, lots of organizations have become deeply dependent on information processing systems. The concluding stage of dependence was reached with the development of e-commerce (Zuccato 2004). This dependency has generated a need for protecting computer systems by means of information systems security. Security requirements ought to be used to describe what kind of security level an information system needs (Gerber 2000). Integrating sustainability into development of business, investment is the main strategy of current governmental issues. New government guidelines require that the regions combine the advancing together strategy into a single integrated regional framework. That requires information systems to be used widely.
Organizations have been benefiting from information processing systems becoming more and more dependent on it with the introduction of e-commerce in last few years. The use of information technologies has raised the demand for protection of organization's data and business. Therefore, information system security has become an essential part of electronic environment like e-education, e-government, e-commerce etc. The aim of advances in Information technologies is to improve life standards, share information, make social relationships stronger, and help organizations remain competitive in the electronic environment (Zuccato 2004).
E-government is one of areas which information system security has an enormous importance.

E-government uses information technologies in public administration to help citizens access to governmental information, citizen services, businesses and government agencies. It always need to be improved to provide better services and easier ways for participating in democratic institutions and processes like voting.

Therefore, information security becomes main responsibility for e-government where security properties of availability, confidentiality, integrity, accountability and information assurance must be fulfilled (Joshi 2001).

A successful and secure e- government will earn confidence and trust of all users (citizens, businesses, organizations, government). Although it is getting easier to develop online government implementations, security issues are getting bigger with the increasing citizen mobility. By enabling government services to be accessible anytime anywhere is also another challenge to avoid intruders to damage or exploit the system (Dridi 2001).

E-commerce is another area where financial information is exchanged and should be protected. There are notable advances on development of e-commerce applications. Most of the e-commerce applications have being modified to be used in mobile environment. Mobile-commerce (m-commerce) also initiated new researches on mobile applications, devices, and middleware and wireless networks. New applications have been created to be used only in mobile environment (Varshney 2002). Some of mobile commerce applications are mobile advertising, mobile inventory management, product locating, mobile shopping, mobile auction, and wireless data center (Varshney 2002).

The aim of this work is to describe an approach for the importance of the information security for sustainable development. Our main approach is to emphasize security requirements for e-commerce, m-commerce, e-government and e-banking (Mallov 2002).

2. The Need for a Secure Information System

An important issue in information systems is dependability and security. Organizations need secure transmission of a document between two parties over network. For wide area networks, such as Internet, flow of private data has a considerable risk to be stolen. That risk affects the trust on information systems. Business organizations need a secure framework to enlarge their investments. And government lay its applications on trust of the security of citizens' information. Development of every organization is dependent on information security. Security of system for business is not only to enable them to take advantage of new market opportunities but also to protect their assets. They need to develop confidence and trust in the electronic world to continue their activities worldwide. Security concerns can be divided into concerns about access control, and concerns about information and transaction security. These schemes are the basis of several electronic payment and procurement systems, as presented in the following sections.

2.1. E-Commerce Applications

E-commerce server provides sell-side (auction, catalogue), buy-side (catalogue, bid), customer service (customer management, collaboration, and so on), security (access control and authorization), and integration (application middleware) functionality components. Various types of applications and technological devices were developed to support those activities. One of the devices to store digital signatures, fingerprints etc. is smartcards. Smartcards can be programmed to work on multiple applications. They have additional built-in computing capability. Besides, there are supporting systems for transmission of data between two parties. Secured Socket Layer (SSL) is a protocol that handles authentication and encryption for Internet message transmission. The protocol is built into web browsers and operating systems that enables the use of Internet shopping, Internet banking and vice versa. For credit card payments over the Internet, another protocol as Secured Electronic Transaction (SET) is widely used. That protocol uses digital certificates to authenticate transactions. Cybercash is another scheme that ties customer to a particular machine containing wallet and proprietary software. The payment method can be credit card, digital coins or direct debit. Credit cards are useful with secure communications technologies such as SSL. And the smart card readers will accelerate their use on the Internet. For business-to-business (B2B) e-commerce electronic coins and electronic cheques need to be promoted. Another key issue to consider is how to maintain financial transaction records for all parties involved in electronic payments. The issues related to present and future payment methods are complex and it is still too early to know how business will accept and adapt to new electronic payment methods (Greenfield 2000).

2.2. M-commerce Applications

M-commerce is a rising discipline involving applications, mobile devices, middleware, and wireless networks. Most of existing e-commerce applications can be adapted to run in wireless environment. Contrary to e-commerce applications that generally run on fixed network infrastructure, m-commerce applications may not get such dependability from the existing wireless infrastructure. The m-commerce applications consist of mobile financial applications, mobile inventory management, shopping, mobile auction, and wireless data centre (Varshney 2002). If we look into a basic m-commerce transaction and discuss how different m-commerce transactions may be affected by different security vulnerabilities. In addition to security issues related to e-commerce, there are more security concerns related to m-commerce applications (Alisha 2002).

2.3. E-Government Applications

A rapid technological evolution is seen in governmental applications. Therefore that rapid change is not a problem free. E-government is the use of IT in public administration and services for citizens, business companies, and governmental agencies. Security of information systems used is the main concern of that applications. The system has to fulfil the fundamental security properties such as availability, confidentiality, integrity, and accountability and information assurance (Joshi 2001). Thus, a new framework for identifying and organizing the security requirements those are common to all information systems that have been utilized for the development of an integrated on-line e-government platform, are required (Lambrinoudakis 2003).

2.4. E-Learning Applications

In addition to the development, management and offering of on-line courses, the system supports administrative tasks like registration, payments, certification, etc. During the system setup phase, it is expected to ensure that the system must specify the access privileges for all types of users. During the authentication phase, the suitable mechanisms must be engaged for authenticating the identification of all registered users. During the offering the service phase, the integrity and confidentiality of the material provided to and submitted by the students must be ensured. In addition, the proof of origin, submission, delivery and receipt, whenever transactions between students and trainers occur, must be maintained. Moreover, a logging mechanism should be utilized (Lambrinoudakis 2003).

2.5. E-Voting Applications

E-voting supports the transmission of a number of types of election procedures through the Internet. All eligible voters can thus participate in the election. The authentication of voter and election organiser identification is a requirement prior to any type of relations of the user with the system. Even though state officials, will generally be trusted, they must be authenticated before accessing the system and all their actions must be logged. During offering the service phase in which eligible voter can select a ballot and cast her/his vote, there are plentiful essential security requirements (Ikonomopoulos 2002). Some indicative ones are anonymity, confidentiality, integrity, no one can vote twice, etc. The last system phase which refers to the storage of the ballots cast and the calculation of the election tally should be available only after the election process has finished and its aim is to validate votes and determine the total number of votes each candidate has received. Throughout tallying the integrity must be ensured such that the participation and active involvement of party representatives, while logging of all actions is necessary. After the tallying process the votes and other relevant evidence must be stored in a secure way. As a result security issue is also important for e-voting applications (Lambrinoudakis 2003).

3. Security technology for Sustainable Development

As we discussed in the previous section, security must be considered carefully when designing Internet-based systems. Any application must have a security policy, appropriate security mechanisms for its application area and monitoring and auditing mechanisms to examine the system in a secure functionality. Security concerns can be divided into two categories: concerns about access control, and concerns about information and transaction security. Access control mechanisms such as passwords, encrypted smart cards, biometrics and firewalls certify that only legitimate users and applications get access to information resources such as user accounts, files and databases. Information and transaction security schemes such as secret key encryption and public key encryption are used to ensure the privacy, integrity and confidentiality of business transactions and messages. This design is the foundation of numerous electronic payment systems. Different number of practical measures improves security concerns. Firewalls and proxy servers can block undesirable attempt to access the internal systems. Strong authentication mechanisms supply system access only to legitimate users. Access control mechanisms grant users rights to access only the resources and applications they need to do their work. Careful planning and administration of a secure network can diminish the risks of attacks. Defending against the unfamiliar attacks is not possible, but the risk can be mitigated with good system design (Greenfield 2000).

Cryptography is the most important technique which transforms digital information from one format to another based on the value of a number, known as the encryption key. The encryption process is a scrambled version of the message that the recipient can then decrypt, by using either the original key (symmetric encryption) or a different, but related, key (asymmetric encryption). The latter one is known as public key cryptography, relating a pair of keys, one private and one public. Information encrypted using the public key can only be retrieved using the corresponding private key. Furthermore, public and private keys can be used to create and verify "digital signatures". Digital signature is appended to messages to authenticate the message and the sender. In an internet application, a robust public key infrastructure (PKI) is needed to make possible secured and trusted transactions. As a result, this will provide information security framework for sustainable development to generate, store and manage keys and digital certificates, security policies for cryptographic systems used (Greenfield 2000).

4. Conclusions

It has turn out to be obvious that security on the Internet is indeed inadequate for sustainable development. In this paper, we presented various information security requirements for sustainable development. In particular, we discussed the dependability of infrastructure for different e-applications. Due to the open and unconstrained nature of the Internet, staying ahead of hackers is becoming harder if not impossible. If the Internet is to actually be successful as a medium for e-applications, the security-related issues must be addressed. Even if variety of techniques have been discussed to present protection and increase security on the Internet, the techniques are ad hoc fixes and resolve only a small portion of a wide spectrum of Internet security problems. In addition, many of these fixes can be subverted through security holes in other system programs. A solution to the security problem may lie in a result of current techniques, but this may lead to downgrading of quality of service. Conceivably a change in the approaches -applications are written- and in the structure of the Internet are required.

References

Dridi, F. & Pernul, G. & Unger, V. (2001). *Security for the electronic government.* Proceedings of the European Conference on E-Government, Trinity College, Dublin, Ireland September.

Gerber M & von Solms R. (2000). *From risk analysis to security requirements.* Comput Secur;20(7):577e84.

Greenfield, Paul & Maheshwari, Piyush & Brebner, Paul & Gorton, Ian. (2000). *E-commerce security.* Australian National Electronic Authentication Council (NEAC) report. August 2000.

Ikonomopoulos, S. & Lambrinoudakis, C. & Gritzalis, D. & Kokolakis, S. & Vassiliou, K.. (2002) *Functional requirements for a secure electronic voting system.* Proceedings of the IFIP TC11 17th International Conference

on Information Security, Egypt, Cairo (2002) 507–520.

http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6TYP-483442H-3-C&_cdi=5...

Joshi, J. & Ghafoor, A. & Aref, W.G. & Spafford, E.H. (2001)., *Digital Government Security Infrastructure Design Challenges.* IEEEComputer34(2).

Lambrinoudakis, C. & Gritzalis, S. & Dridi, F. & Pernul, G. (2003). *Security Requirements For e-Government Services: A Methodological Approach For Developing A Common PKI-Based Security Policy.* Computer Communications, Vol. 26, No. 16, pp. 1873-1883, Elsevier

Malloy, Alisha D. & Varshney, Upkar & Snow, Andrew P. (2002). *Supporting mobile commerce applications using dependable wireless networks, Mobile Networks and Applications*. v.7 n.3, p.225-234, June 2002

Varshney, U. & Vetter, R.. (2002). *Mobile commerce: Framework, applications and networking support.* Mobile Networks and Applications 7 185–198.

Zuccato, Albin. (2004). *Holistic Security Requirement Engineering For Electronic Commerce.* Computers & Security 23(1): 63-76.