E-commerce Systems and E-shop Web Sites Security

Suchánek, Petr

Silesian University - School of Business Administration

24 March 2009

E-commerce Systems and E-shop Web Sites Security

Petr Suchánek
The Silesian University, School of Business Administration in Karviná, Department of Informatics
E-mail: suchanek@opf.slu.cz

Abstract

Fruitfulnes of contemporary companies rests on new business model development, elimination of communication obstacles, simplification of industrial processes, possibilities of responding in real-time and above all meeting the floating custom needs. Quite a number of company activities and transactions are realized within the framework of e-business. Business transactions are supported by e-commerce systems. One of the e-commerce system part is web interface (web sites). Present trend is putting the accent on security. E-commerce system security and web sites security is the most overlooked aspect of securing data. E-commerce system security depends on technologies and its correct exploitation and proceedings. If we want e-commerce system and e-shops web sites with all services to be safety, it is necessary to know all possible risks, use up to date technologies, follow conventions of web sites development and have good security management system. The article deals with definition and description of risk areas refer to e-commerce systems and e-shop web sites and show fundamental principles of e-commerce systems and e-shop web sites security.

Keywords

E-commerce system, e-shop web sites, security, security proceedings, web technologies.

Introduction

E-commerce is the online transaction of business, featuring linked computer systems of the vendor, host, and buyer. Electronic transactions involve the transfer of ownership or rights to use a good or service. E-commerce includes retail shopping, banking, stocks and bonds trading, auctions, real estate transactions, airline booking, movie rentals-nearly anything we can imagine in the real world. Capital assets of e-commerce are internet shops (e-shops). E-shops are realized as web sites with many services. In the Czech Republic the first e-shops were developing since 1995. At that time e-shop web sites were not enough safe and contained small number of user-friendly services because of absence of web sites developer experiences and knowledge and technological possibilities. Nowadays modern technologies make web sites developers possible to create intuitive, elegant and user-friendly web sites with great number of safed services.

Internet and information technologies brought new possibilities but also risks. Internet will never be 100 % safe as well as anything. Well-formed risk management and exploitation of modern information technologies in connection with base of knowledge form secured environment to support safe data transfer during system communication.

1 Conditions of Efficient E-commerce System

E-commerce belongs to e-business activities in firms. Implementation of e-business requires detailed analysis and strategic concept development. In e-business strategy must be taken in firm structure, firm produce and business activities, target group, competition, return on investments, technical support, personnel, system of security, risk management, operating system, management system, etc. Individual parts may be under consideration and analyzed at successive steps or in parallel with regards to contexture. [2] Security area and risk management has to be analyzed in detail. E-business strategy has to always be fundamental element. Wrong or incomplete analysis can be the causes of problems especially refer to increasing of investments to a new analysis or system re-engineering.

E-Shop means the sales outlet of the Company on its website. If we want e-commerce activities realized by e-shop to be efficient, many conditions have to be fulfilled. As conditions we can consider:

- return on investment (ROI),
- big profit,
- advanced edit tools (for administration and publicity),
- easy operation (for customers and administrative staff),
- unit construction,
- rate,
- stability,
- security,
- perfect design,
- well-arranged navigation,
- customer interface,
- supplier interface,
- low service costs,
- personification,
- multishopping (keeping of number of e-shops web sites).

Direct dependence on e-shop security results from historical e-commerce development. At the beginning customers was afraid of electronic shopping security. In a way they were right because of absent of web developer experiences and sufficient sophisticated technologies. Actual state of affairs is different and interest in e-commerce is increasing all the time. People more and more use Internet and its services and generally Internet happened standard part of life.

2 E-commerce System Security

E-commerce system is an electronic system that automates the exchange of goods and services over the Internet in a secure environment. E-commerce systems security is more exacting for reasons of necessity to connection internal and external processes. Creating an infrastructure to protect a company, its trading partners, and its customers is crucial if businesses are realized the full potential of the Internet.

Earlier then we will define main fundamentals of e-commerce, we should answer to many question and answers should be main home elements of corporate e-commerce strategy. As questions can be introduced for example what components are most critical but vulnerable, what information is confidential and needs to be protected, how will confidentiality be ensured, what authentication system should be used, what intrusion detection systems should be installed, who has authority and responsibility for installing and configuring critical e-business infrastructure, what plans need to be in place to ensure continuity or minimum disruption of service etc. [1]

E-commerce systems are transaction processing systems. Transaction processing systems security is based on two fundamental conditions:

- **Authentication** – user is who he says he is.
- **Authorization** – definition of what is an authenticated user allowed to do.

Authentication and authorization saves systems against illegal ways of usage. With regard to global of Internet, hackers can do attack from any places in the world. In term of time heftiness attack may be done within seconds but it may result in big damages and financial loss. Result from research, many attacks on information systems are made from internal environment. In many cases employees did active attack but even problems were evoked by user mishandling with information system. In this respect we do not have to forget on illegal way of user working with information system caused, for example, by not knowing of users. On this account information system has to be secured not only against hackers (active, planned attacks) but also against improper user actions.

In e-commerce systems security has to be ensured especially in context of:

- system of payment,
- server attacking,
- protection of name of description,
- other specifications associated with e-business transactions on internet.

2.1 System of payment

Nowadays development and operation of safe electronic payment system is not in term of technologies grand problem. Main reason is standardization of technologies. Quality payment system has to fulfil the conditions:

- **Maximum security ensuring** – securing of all data flows by virtue of HTTPS (SSL certificate) and server against abuse. Pivot element is pay card verification by virtue of 3D Secure (attestation in three different places). Verification is done on bank servers (outside web server of seller).
- **Detailed consumer awareness** – system supply to customers supporting information about all steps of business transaction. It assists to increase custom trust.
- **Easy operation** – for everyone and especially for less experienced users.
- **Integration of payment system and other information systems** – integration of payment system with ERP, CRM, Business intelligence etc. It assists to fast and efficient transaction processing on seller side. Integration is very important condition.

In term of users, security of payment systems is more important then everything else. At present small number of people in working age do not have bank account with electronic banking possibility. In classic e-shops people very often use possibility to pay by cash on delivery. It relates to other type of risk namely to do not pay for goods in advance but after as much as procurement. At the level of B2B, using of cash on delivery is impossible in the majority of cases. Just especially level B2B demands sophisticated and protected electronic payment systems.

2.2 Server attacking

E-commerce systems, especially e-shops communication technology is based on client/server architecture (Fig. 1). In client/server architecture access, resources, and data security are controlled through the server

(centralization), any element can be upgraded when needed (scalability), new technology can be easily integrated into the system (flexibility) and all components (clients, network, servers) work together (interoperability).

In terms of customers doing business in e-shop there is need to ensure data transfer in between client and server. Data are passwords (submitted during registration or login), name and descriptions (for example during order writing) etc. This type of data has to be ensured during data transfer on Internet network. Main question is how are we able to ensure data so that it could not be caught and abused.

A secure web site uses encryption and authentication standards to protect the confidentiality of web transactions. Currently, the most commonly used protocol for web security is SSL, or Secure Sockets Layer. In addition to providing security for HTTP (web hypertext) transactions, SSL works with other TCP/IP standards such as IMAP mail and LDAP directory access. For a security standard such as SSL to work, browser and the web server must both be configured to use it.

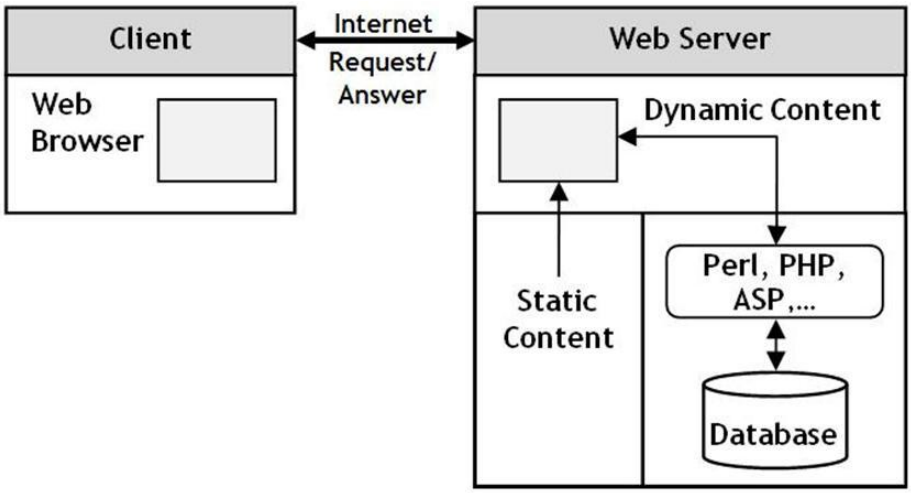

Figure 1 Client/server architecture of e-commerce system.

Many SSL Certificate vendors (Verisign, GeoTrust, SSL.com, etc.) also provide a "site seal" to the owners of these web sites. Common characteristics of these site seals include [6]:

- **High Visibility** - Online merchants want you to see these site seals. They want you to know they have made every effort to make their site a safe shopping experience. Therefore, the site seal is usually located where you, the customer, can easily see it.
- **Difficult to Duplicate** - The site seals are designed to be difficult for thieves and scammers to duplicate. Many times the site seal will have a date and time stamp on it.
- **Verification Functionality** - The site seal should have some functionality whether by clicking on the seal or by hovering your mouse over the seal. The functionality should display detailed information about the web site you are visiting.

Number of server attacking increase all the time. New methods of server attacking appear and web developers have both hands full of work with searching of new security technologies. Web developers have to do everything to protect information system and e-commerce system against unauthorized use, hacking and dangerous software (computer virus, spyware, adware, etc.).

Resulting from research and statistics, since many organizations (especially small and middle sized firms) do not monitor online activity at the web application level and hackers have free reign and even with the tiniest of loop holes in a company's web application code. Any experienced hacker can break in using only a web browser and a dose of creativity and determination. It is very necessary to take control and filter of all custom requests.

In simple systems web interface is often abused for an attack of internal information system. Main way of internal system security is good definition of system architecture and exploitation of firewall. As standard should be, important servers (database servers, servers of ERP, CRM, BI etc) are usually located in demilitarized zone (Fig. 2). With reference to e-commerce system extensiveness, externalization, target group and last but not least pocket book there are number of system architectures ensuring smaller or higher safeguard against external and internal attacks.

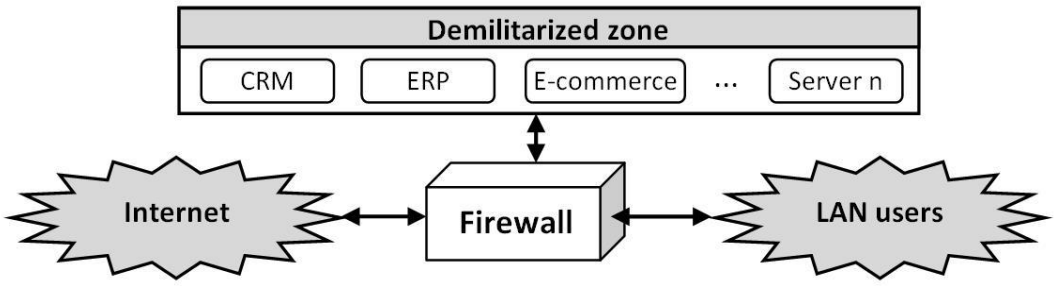

Figure 2 Demilitarized zone of servers.

Introduced architecture protects servers not only against external hackers but also against local users. In e-commerce systems we have to solve problem respecting place of web server that is main interface. Also in this case we can use system architecture with two demilitarized zones (Fig. 3). This and other modifying architectures are used in many cases in different systems, for example Microsoft Dynamics NAV.

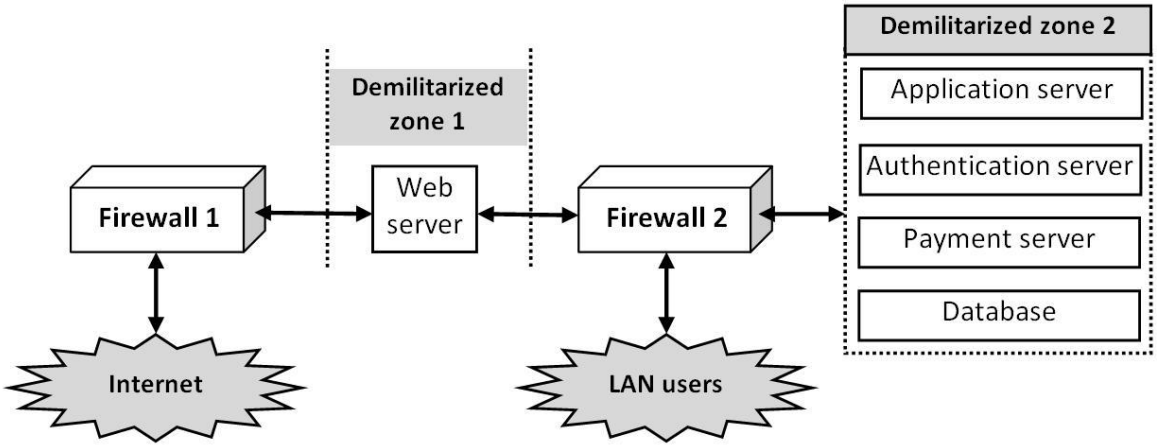

Figure 3 Web server standalone in demilitarized zone.

System architecture, number of firewalls, number of servers etc. depend on required purpose, e-commerce system software, required factor of safety, financial competence etc. System architecture should come from corporate strategy because of the minimization later needs of changes. Every system modification usually results in greater system changes implied originally and heavy investment. In some cases for example server with CRM system can be faulted in demilitarized zone 1 shown in Figure 3.

2.3 Protection of name and description

Common internet user browsing web sites very often need to afford name and description. In many cases if he wants to get some information or buy anything in e-shops, he has to supply any name and description. Protection of name and description rests on technologies and its properly using and human element. The rule is that people should be very careful and fill name and description only on serious web sites forms (for example goods order, ticket booking, tour booking, air ticket booking etc.). If user checks in other type of non-serious web sites such may be game sites, web sites with delicate content or other types of private web sites, he has to take any risks into account.

2.4 Secured E-shop Web Sites

E-shops are realized and presented as web sites. Security is by one of main conditions of efficient e-shops. E-shops web pages are only one point of e-commerce system.

Matter of principle is determination of term secured web sites. How can we find secured web sites? There are two general indications of secured web sites [7]:

- **Check the web page URL** - normally, when browsing the web, the URLs (web page addresses) begin with the letters http. However, over a secure connection the address displayed should begin with https.
- **Check for the Lock icon** - there is a de facto standard among web browsers to display a lock icon somewhere in the window of the browser.

E-hop web sites can be considered as secured if:

- they are not able to be changed by hackers easily,
- hackers cannot get user name and description,

- hacker cannot change price size in payment system,
- hackers do not have random access into information system through e-shop web sites,
- user get goods or services on order all right and in good time,
- after registration and writing name and descriptions users do not get spam and other e-mails from unknown senders.

2.5 Ways of e-commerce system attack

If we want to prevent of e-commerce system attack, we have to know ways of attacks. About every set forth bellow types of attacks could be write a book but it is necessary for web developers and server administrators to know its.

- **Background** – hacker changes background of e-shop web sites.
- **SQL Injection** - is subset of the unverified/unauthorized user input vulnerability and the idea is to convince the application to run SQL code that was not intended. Hacker can gain access to protected data, user´s accounts, delete data in tables etc.
- **Price Manipulation** – hackers are able to change prices in e-shop, in order or in payment order.
- **Buffer overflows** - is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations.
- **Cross-site scripting** - (XSS) occurs when an attacker introduces malicious scripts to a dynamic form that allows the attacker to capture the private session information.
- **Remote command execution** - command execution refers to attackers attempting to use an existing website to execute OS commands on a web server. By inserting system level commands into an HTTP request to the target web server, users may be able to execute system level commands, create system faults, or steal sensitive information from your system, if security holes exist.
- **Weak Authentication and Authorization** – hackers are able to gain access to information system and read, rewrite or delete data.
- **Viruses** – hacker sends viruses to corrupt business data.
- **Spamming** - is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

There are many methods and technologies to help server and network administrators and web developers to protect systems against above-mentioned ways of attacks. Development of secure technologies is fast enough and overwhelming majority of secure technologies is ne plus ultra. At present breaking-through system probability is decreasing all time but it doesn´t mean that technologies are 100 % safe. Technologies have to innovate all time.

2.6 Methods of E-commerce System Protection

Methods of e-commerce system protection are the same as generally methods of protection used in information system (Table 1). Attacks can be accidental or well-considered done with target to take away data or damage goodwill. As accidental attacks we can mark for example unknowingly program (containing virus) start by user. In many cases attacks were done by LAN users (internal environment). This problems would deserve independent article contain detailed analysis. In this case main protection is legislature, employee motivation and their firmness. Of course architecture and all parameters of information system should be adjusted so that each of unchartered or suspicious user´s steps would be found out in time.

Method	Description
Data backup	Data backup is main condition of efficient and safe information system. Data backup have to be realized so that all data have to be renewable from backup.
Antivirus and anti-spyware protection	Antivirus and anti-spyware protection have to be applied to individual computers and servers.
Important data security	All data in information system should be considered as important, but it may be defined special groups of data expected enhanced security. It is necessary to define policy of privacy keys.
Periodic audit	All the time system monitoring has to be doing and in regular time interval periodic audit ensure compliance of all fundamentals of information system work.
Anti-spam	Exploitation of acceptable software and its correct adjustment especially on the server level.
Firewall and proxy server	Main interface in the midst of firm internal and external environment.
System monitoring	Checking of unnormalized events and detection of security incidents.
User training	User training is contributing to enhancement of user knowledge and responsibility.

Table 1 Methods of e-commerce system protection and its description.

3 E-commerce System Security Proceedings

Generally, security should be considered by one of the most important condition of successful business transactions. One of the important conditions of e-commerce system security is good management system. Management system should contain the set of functions that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences and that includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms.

Every system has to have defined management strategy and its support of information system. From management strategy results changes of information systems or its complete innovation. Management systems have to be conceived on the basis of processes needs in connection with their support of computer technology. It ensures source information to be attended in good time and right place. [3]

We are able to model management system of e-commerce system security with usage of control circuit (Fig. 4). Control circuit can be applied for modeling of many other firm modules.

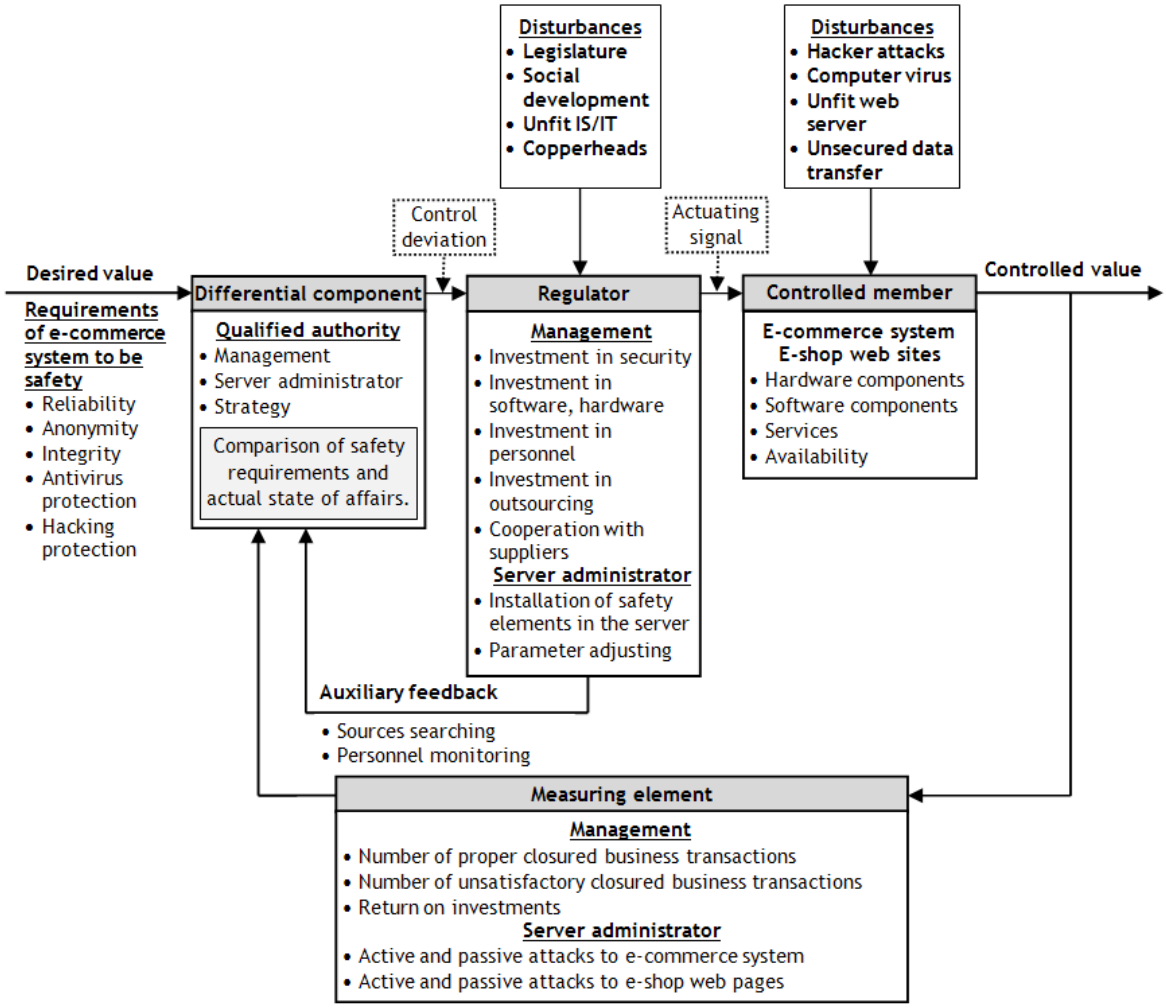

Figure 4 E-commerce system security proceedings.

To faultless of e-commerce system is necessary continuous monitoring and feedback. Main feedback is observed by measuring element, but very important is auxiliary feedback which makes possible higher-speed response. Shown management model is able to help with control of security and supply very important fundamental information of security system development.

4 Web Standards as Condition of Security Web Sites

Web standards is a general term for the formal standards and other technical specifications that define and describe aspects of the World Wide Web [4]. We can meet many opinions about web standard but it stands that many standards result from historical internet development. It stands to reason, using modern technologies and standards by all web developers and e-commerce systems contribute to system security increasing. As last part of article I write enumeration of fundamental methods, technologies, languages etc. used for web sites development (Table 2).

Methods, technologies, languages, …	Description
HTML (Hyper Text Markup Language)	HTML is used only for web page structure definition and fundamental text formatting. At present web sites contain many services had to be realized by other programming languages with the support of various types of databases, query languages, protocols and so on. Only service can be realized with support of HTML is e-mail. HTML by itself is not close support of web pages security.
XHTML (Extensible HyperText Markup Language)	XHTML first came along in December of 2000. XHTML is a family of current and future document types and modules that reproduce, subset, and extend HTML 4. XHTML 1.0 (this specification) is the first document type in the XHTML family. It is a reformulation of the three HTML 4 document types as applications of XML 1.0. Unlike HTML, all XHTML have to have a closing tag. Because XHTML documents are written according to the rules of XML, it is not difficult for XML-processing programs to convert an XHTML file to another format (e.g. PDF, RSS or RTF). XHTML with support of CSS enable development of semantic right structured document in which contain and design are separated. Main advantages are right semantic structure of document, superior and more extensive possibilities of formatting, nearly 50 % faster www pages loading, smaller file size of web page, faster rendering, back compatibility with HTML, compatibility with more internet browsers, quality printout.
XML (EXtensible Markup Language)	XML is an open standard for describing data from the W3C. It is used for defining data elements on a Web page and business-to-business documents. There are many advantages to using XML for information exchange, and they offer many benefits to the user. The Extensive Markup Language uses human language, which is conversable and not the language used by computers which is binary and ASCII coded. XML is readable by even people who have had no formal introduction to XML or have been coached on it.
CSS (Cascading Style Sheets)	CSS is a stylesheet language used to describe the presentation of a document written in a markup language. Prior to CSS, nearly all of the presentational attributes of HTML documents were contained within the HTML markup. CSS allows authors to move much of that information to a separate stylesheet resulting in considerably simpler HTML markup. All font colors, background styles, element alignments, borders and sizes had to be explicitly described, often repeatedly, within the HTML.
XSLT (Extensible Stylesheet Language Transformations)	XSLT is an XML-based language used for the transformation of XML documents into other XML or "human-readable" documents.
RDF (Resource Description Framework)	RDF is a general framework for describing a Web site's metadata, or the information about the information on the site.
DOM (Document Object Model)	DOM is the specification for how objects in a Web page (text, images, headers, links, etc.) are represented. The DOM defines what attributes are associated with each object, and how the objects and attributes can be manipulated. Dynamic HTML (DHTML) relies on the DOM to dynamically change the appearance of Web pages after they have been downloaded to a user's browser.
SVG (Scalable Vector Graphics)	SVG is a vector graphics file format that enables two-dimensional images to be displayed in XML pages on the Web. Vector images are created through text-based commands formatted to comply with XML specifications. In contrast to JPEG and GIF images on the Web, which are bitmapped and always remain a specified size, SVG images are scalable to the size of the viewing window and will adjust in size and resolution according to the window in which it is displayed.
SGML (Standard Generalized Markup Language)	SGML is a language for defining markup languages such as HTML and for specifying the rules for tagging elements in a document. SGML itself is not a markup language; rather, it is a language to create markup languages.
MathML	MathML is intended to facilitate the use and re-use of mathematical and scientific content on the Web, and for other applications such as computer algebra systems, print typesetting,

	and voice synthesis. MathML can be used to encode both the presentation of mathematical notation for high-quality visual display, and mathematical content, for applications where the semantics plays more of a key role such as scientific software or voice synthesis.
RSS (Really Simple Syndication)	RSS is an XML-based format for content distribution. Webmasters create an RSS file containing headlines and descriptions of specific information. While the majority of RSS feeds currently contain news headlines or breaking information the long term uses of RSS are broad.
Screen reader	Always more often used technology. It is a software application that attempts to identify and interpret what is being displayed on the screen (for example audio). It is useful to handicap people.

Table 2 Table of fundamental web languages, technologies and methods.

Shown standards is necessary used with appropriate database systems, scripts languages and generally specific information system, strictly speaking e-commerce system and its part of ERP, CRM, BI etc. parts. All have to be created as uniform integrated system.

Conclusion

The main aim of article was referred to key areas of e-commerce systems and e-shop web sites security. At present e-commerce systems with web interfaces are of high account part of business systems. Because of the web interface and global structure of internet e-commerce systems have to be secured. Security is important condition of e-commerce system effectiveness just after efficiency. Security has to be defined and analyzed in detail in corporate strategy. E-commerce systems have to have good system architecture, use acceptable software and hardware, be efficient, have secured system of payment, protection against server attacking, protection of name of description etc. All safety codes have to be adjusted with regard to web interface (web sites). To e-commerce system would be saved, system administrator, web developers and top executives should know possible risks and methods of information system protection. If we want e-commerce system to be saved and secured, it has to be in being efficient management system. We are able to model management system of e-commerce system security with usage of control circuit. Crucial condition of e-commerce management system is feedback. Parts of e-commerce systems are e-shop web sites. In this respect web sites security plays an important role in security of whole e-commerce system. Web sites security can be achieved by using of up-to-date web technologies and its correct usage. We do not have to forget to improve qualification of employees, server administrators, web site developers etc. and generally increasing of security needs awareness.

References:

[1] OTUTEYE, E. A *systematic approach to e-business security*. Faculty of Administration, University of New Brunswick, Fredericton, Canada. 2003. [on-line 20.1.2009] http://ausweb.scu.edu.au/aw03/papers/otuteye/paper.html

[2] SUCHÁNEK, P. *E-business Development Key Areas.* In 5-th International Symposium on Business Administration. Çanakale: Çanakale Onsekiz Mart University, 2008. s. 537-543. ISBN 978-975-8100-78-1.

[3] VYMĚTAL, D. *Projekty informačních systémů v podnicích a jejich realizace*. SU OPF Karviná, 2008. 122 p. ISBN 978-80-7248-477-5.

[4] http://www.w3.org

[5] http://www.webrichtlijnen.nl/

[6] http://www.webopedia.com

[7] http://info.ssl.com/article.aspx?id=10068