Influence of Security Measurements on the Quality of Services of MapServer

KOMARKOVA JITKA, HUB MILOSLAV, ULRICH MARTIN
Institute of System engineering and Informatics
University of Pardubice
Studentska 84, 532 10 Pardubice
CZECH REPUBLIC

Abstract: - Internet based geographic information systems (GIS) and so called GIservices have become and inherent and common part of information systems in public and private sector. It means that many new quality requirements on them have risen. Extended ISO/IEC 9126 quality model is chosen for evaluation of some quality sub-characteristics of the chosen Internet based GIS solution. End-user response time and presence or absence of selected security measurements belong to the metrics used for evaluation of the chosen software quality. Influence of selected security measurements on end-user response time was studied on the case of University of Minnesota MapServer. Various security measurements were used for testing purposes, e.g. IPsec protocol, Authentication Header, Encapsulating Security Payload, Secure Sockets Layer protocol, and various encryption algorithms. It was determined that some of the chosen security measurements have a significant influence on the end-user response time.

Key-Words: - Internet geographic information systems, GeoWeb, end-user response time, software quality, security

1 Introduction

Geoenabling the Web and providing so called GIservices to the end users belong to the contemporary development trends in the field of geographic information systems (GIS). Internet and mobile solutions are spreading rapidly over the Internet. For many people it has become normal to use their services, e.g. searching the shortest/fastest route, realty, and many others [1, 2]. Internet based GIS solutions can be now understood as a common software tools and a common part of institutional information systems. Thus, they are widely spread over the whole world. Another reason of the growth of an importance of Internet based GIS solutions is a spreading of ideas of information society in EU countries and the Czech Republic [3]. Geoenabled portals have become inherent parts of Internet/intranet based information systems and applications which are now run as a part of e-government services too [4]. But in the Czech Republic there is problem with slow implementation of e-government services as it was measured by means of the two benchmarking tools [5]. At the same time their data should be shared and become a part of a regional data warehouse which is suitable even for smaller municipalities and which can even provide a fuzzy approach in enquiries [6].

This development has resulted into many new requirements for the quality of provided services and functionality of Internet based GIS solutions. The first requirement is connected to another significant contemporary problem – a fast searching for information on Internet. Agent technologies have been more and more used for this task. Unfortunately, Czech language uses many specific features (e.g. some characters are used with special signs) which must be considered [7].

A part of results of a research dedicated to the quality of service of Internet GIS and their utilization in the Czech public administration are described in the paper.

2 Problem formulation

Solutions of geographic information systems based on Internet technologies and run in the computer networks environment are now a usual part of enterprises and governmental information systems. It means that quality requirements on common information systems are now applied on Internet GIS.

Now we get to the topic of this paper. Geodata and GIservices are provided as a part of e-government services by means of Internet based GIS solutions. The same do private companies – they use this kind of GIS as an inherent part of their production systems. It results into growing dependency on the geographic information system so a high quality of the solutions is required. It means that system functions well, it is reliable, easy to use, etc. Because of the intranet/Internet nature of these solutions, efficiency, security and availability belong to the characteristics of required quality [8].

Presence of security measurements is necessary today. But the security measurements can highly influence availability of services. There are presented results of on-going study in the paper. Influence of selected security measurements on the time of response of selected Internet based GIS solution will be evaluated.

3 Methodology

Dealing with quality of services provided by Internet GIS solutions mans that at first quality model must be defined. There is one commonly used quality model standardized by ISO/IEC: ISO/IEC 9126 - Information technology - Software Product Quality. This model is used for both measuring architectures and intranet applications [8, 9].

As far as a quality model represents quality requirements from a specific point of view, many models exist and any specialist can propose his/her own quality model [10]. For the purpose of this study extended ISO/IEC 9126 model with six basic quality characteristics and refined sub-characteristics [8] will be used. In this model security is used as a sub-characteristic of functionality and time behavior is used as a sub-characteristic of efficiency. These two sub-characteristics are understood as very important ones [8]. Only presence or absence of security measurement will be used as a metric for security for the first stage of study. End-user response time will be used as a metric for time behavior. Influence of particular security measurements on end-user response time will be experimentally measured. For each security measurement 20 measures will be done. End-user response time will be measured with precision of milliseconds. Obtained results will be processed by means of statistical methods.

4 Quality of software and quality models

At first, the term quality itself must be defined in a usable way. Quality is defined as "conformance to requirements" and "fitness for use" [11] for the purpose of this research and paper. The first part - "conformance to requirements" – means that all the requirements must be stated clearly and in a measurable way. The second part - "fitness for use" - means that users view and expectations must be taken into account [11].

Each quality model describes quality by means of a set of characteristics at various level of abstraction and at the same time it shows relationships between characteristics. There are many software quality models, e.g. Boehm model, McCall model or newer ISO/IEC 9126 one. According to ISO/IEC 9126 model it is possible to refine each quality characteristic into multiple levels of sub-characteristics [10].

The process of a software design is understood as a very important phase with the key influence on software quality. Both traditional and agile approaches have some advantages and disadvantages and can influence on the resulted software quality [12]. Regardless of the importance of system design this topic will not be covered by this paper.

5 Problem solution

University of Minnesota MapServer was chosen as a server part of Internet based GIS solution. It is based on client/server architecture. Linux was chosen as an operating system on both server and client side.

As first it is necessary to choose a proper quality model. Extended ISO/IEC 9126 model is used as a basis for evaluation of efficiency of selected Internet GIS solution.

5.1 Software quality model and used metrics

As it was stated, in this case it was decided to use extended ISO/IEC 9126 model which was found as a suitable one for intranet applications [8].

The first used sub-characteristic is **security** and a presence or absence of security measurement is used as a metric. The first set of measurement was done with absence of a security measurement. Then following security measurements were tested:

- Packet filtration – **http-filtr**
- Internet Protocol Security (IPSec), Authentication Header (AH), check sum (HMAC) calculated by means of MD5 algorithm (128 bits), transport regime – **http-ipsec-ah (transport-MD5)**
- IPSec, AH, SHA2 (168 bits), transport regime – **http-ipsec-ah (transport-SHA2)**
- IPSec, AH, MD5 algorithm (128 b), tunnel regime – **http-ipsec-ah (tunel-MD5)**
- IPSec, AH, SHA2 (168 b), tunnel regime - **http-ipsec-ah (tunel-SHA2)**
- Internet protocol security (IPSec), Encapsulating Security Payload (ESP), data encryption by means of AES256 algorithm (256 b), check sum calculated by means of MD5 algorithm (128 b), transport regime – **http-ipsec-esp (transport-aes256-md5)**
- IPSec, ESP, Blowfish128 (128b), MD5 (128b), transport regime – **http-ipsec-esp (transport-blowfish128-md5)**
- IPSec, ESP, AES256, MD5, tunnel regime - **http-ipsec-esp (tunel-aes256-md5)**
- IPSec, ESP, Blowfish128, MD5, tunnel regime - **http-ipsec-esp (tunel-blowfish128-md5)**
- Secure Sockets Layer (SSL), Diffie-Hellman algorithm (DHE) for key exchange, authentication protocol: RSA (length of private key: 1024 bits), data encryption by means of AES256 algorithm (256b), check sum (HMAC) calculated by means of SHA1 (160 b) – **https (DHE-RSA-AES256-SHA)**
- SSL, RSA (1024b), RSA (1024b), AES256,

SHA1 – **https (RSA-RSA-AES256-SHA)**

- SSL, DHE, RSA, AES256, SHA1 + IPSec, ESP, Blowfish128, MD5, tunnel regime – **https (DHE-RSA-AES256-SHA + ipsec-esp-tunnel-blowfish128-md5)**.

The second sub-characteristic is **time behavior**. A real end-user response time is used as a metric in this case. It is measured in seconds on the client side as a real time between sending the user's command to obtaining the result from the server.

5.2 Experimental measurements and results

Measurements were run on the following computers: server configuration: Intel Celeron (Coppermine) 600MHz, MB MSI 6309 (VIA 694x), 384MB SDRAM 100MHz, HDD Seagate 60GB 5400 rpm, Edimax 9130TXA PCI with Realtek 8139d chip (100Mbps, full duplex), operating system Debian GNU/Linux 3.0r1 with kernel 2.4.19, Apache HTTP Server 2.0.47, MapServer 4.0.1.

Client configuration: AMD Athlon XP-1700+, MB ECS K7VTA3B (VIA KT333), 256MB DDR 266 MHz, HDD Western Digital 80GB 7200 rpm, Edimax 9130TXA PCI with Realtek 8139d chip (100Mbps, full duplex), operating system Debian GNU/Linux 3.0r1 with kernel 2.4.19.

Measurements were done in an environemnt of real computer network.

Obtained experimental results, i.e. 20 response times for each security measurement, were statistically treated. The first part of the results of the statistical treatment (average end-user response time and standard deviation) is listed in the Table 1 and shown on Fig. 1.

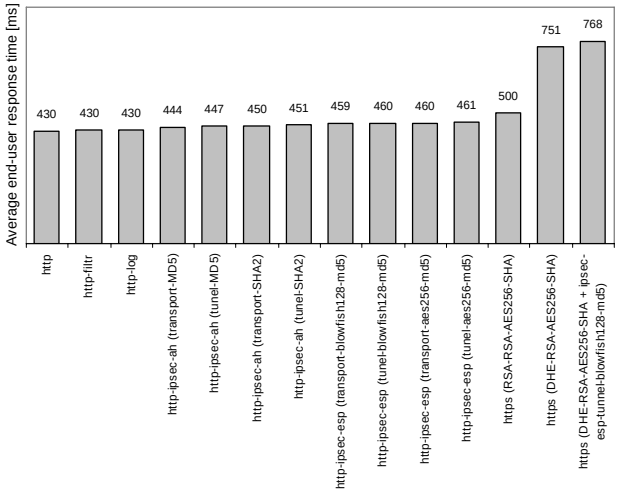

Fig. 1 – Average response time

Table 1 – Average response time and standard deviation for selected security measurements

Security measurement	Average response time [ms]	Standard deviation [ms]
http	430	2,24
http-filtr	430	0,01
http-log	430	5,03
http-ipsec-ah (transport-MD5)	444	0,01
http-ipsec-ah (tunel-MD5)	447	4,89
http-ipsec-ah (transport-SHA2)	450	2,24
http-ipsec-ah (tunel-SHA2)	451	0,01
http-ipsec-esp (transport-blowfish128-md5)	459	3,66
http-ipsec-esp (tunel-blowfish128-md5)	460	2,24
http-ipsec-esp (transport-aes256-md5)	460	2,24
http-ipsec-esp (tunel-aes256-md5)	461	0,01
https (RSA-RSA-AES256-SHA)	500	2,24
https (DHE-RSA-AES256-SHA)	751	5,5
https (DHE-RSA-AES256-SHA + ipsec-esp-tunnel-blowfish128-md5)	768	0,01

A relative comparison of obtained results is shown on the Fig. 2. Obtained end-user response times are related to the response time of MapServer when no security measurement is present (http protocol).

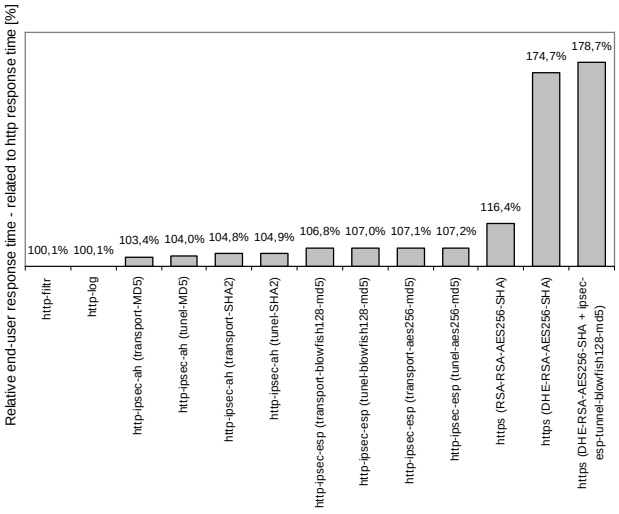

Fig. 2 – Relative response time – related to http response

Average server processing times and transmission times for each security measurement are shown on the Fig. 3 and Fig. 4.

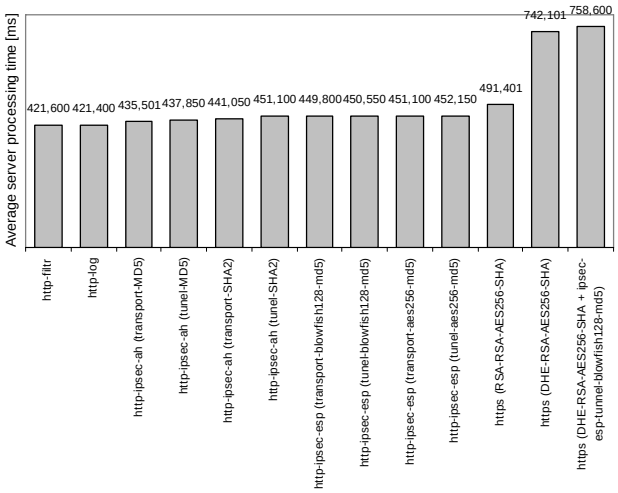

Fig. 3 – Average server processing time

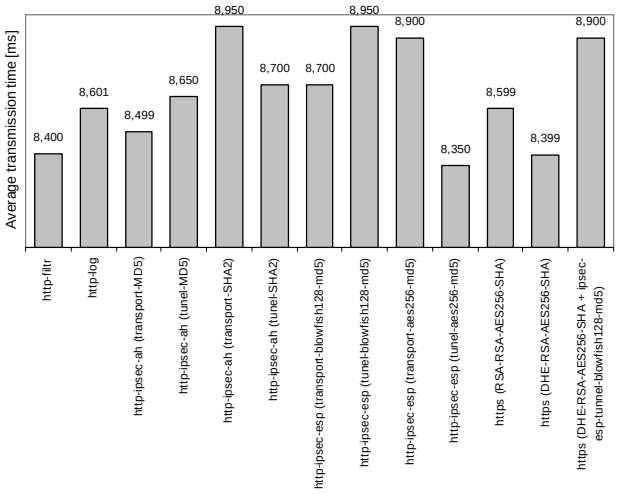

Fig. 4 – Average transmission time

6 Conclusion

Internet based GIS solutions have become a widely used and inherent part of information systems both in private and public sector. Their expansion is driven by the increasing demand for geodata and GIservices by the end-users.

This fact results into increasing quality requirements on these solutions. Many quality models can be used for evaluation of the software quality. In the case of this study, extended ISO/IEC 9126 model was chosen because it was found as a suitable one for intranet applications [8].

During the experimental work it was found that utilization of HTTPS protocol causes longer end-user response time of MapServer. The response time has an extension of 16% when RSA algorithm is used and more than 70% when Diffie-Hellman algorithm is used for key exchange. For the future it is proposed to increase number of measurements and to increase a precision of the measurements, i.e. to use microsecond as a unit.

References:

[1] Peng, Z.-R., Tsou, M.-H., *Internet GIS: distributed geographic information services for the internet and wireless networks*, John Wiley & Sons, 2003.

[2] Longley, P., A., *Geographic information systems and science*, John Wiley & Sons, 2001

[3] - The Office of the CR Government -, Available from http://www.vlada.cz/1250/eng/vrk/rady/sip/dokumenty/sipcesta/sip.eng.html

[4] Capek, J., Using ICT technology within region managing focusing to waste recycling control. *WSEAS TRANS. on INFORMATION SCIENCE and APPLICATIONS*, Vol. 1, Nr 5, 2004, pp. 1389 - 1393

[5] Kopackova, H., Measuring e-Government – The Czech Republic in the View of International Evaluation Methods, *WSEAS TRANSACTIONS on INFORMATION SCIENCE AND APPLICATIONS*, Vol. 1, Nr. 5, 2004, pp. 1277 - 1282

[6] Simonova, S., Capek, J., Fuzzy Approach in Enquiry to Regional Data sources for Municipalities, *WSEAS TRANSACTIONS on SYSTEMS*, Vol. 3, Nr 2, 2004, pp. 823 - 827

[7] Janakova, H., Text categorization with feature dictionary problem of Czech language, *WSEAS TRANSACTIONS on INFORMATION SCIENCE AND APPLICATIONS*, Vol. 1, Nr. 1, 2004, pp. 368 - 372

[8] Leung H., K., N., Quality metrics for intranet applications, *Information & Management*, Vol. 38, Nr. 3, 2001, pp. 137 – 152

[9] Losavio, F., at all, ISO quality standards for measuring architectures, *The Journal of Systems and Software*, Vol. 72, Nr. 2, 2004, pp. 209 – 223

[10] Azuma, M., Software products evaluation system: quality models, and processes – International Standards and Japanese Practice, *Information & Software Technology*, Vol. 38, Nr. 3, March 1996, pp. 145 – 154

[11] Kan, S., H., *Metrics and Models in Software Quality Engineering*, Second Edition, Addison Wesley, 2002, ISBN 0-201-72915-6.

[12] Fernandes, S., M, Belix, J., E., Melnikoff, S., S. S., Spina, E., Confronting Antagonistic Views of Software Design, In *Proceedings of the WSEAS Conference System Science and Engineering (ICOSSE 2005)*, ISBN: 960-8457-18-1, Avaliable from http://ns.snd.edu.gr/wseas/wetsi/2005brazil/papers/494-223.pdf