International Journal of Pharmacology

ISSN 1811-7775

science alert

ansinet
Asian Network for Scientific Information

International Journal of Pharmacology 6 (6): 959-964, 2010
ISSN 1811-7775

Suitability of Using SOAP Protocol to Secure Electronic Medical Record Databases Transmission

[1]Mohamed Shabbir A. Nabi, [1,4]M.L. Mat Kiah, [2,4]B.B. Zaidan, [2,4]A.A Zaidan and [3]Gazi Mahabubul Alam
[1]Department of Computer System and Technology,
Faculty of Computer Science and Information Technology, University of Malaya,
50603 Kuala Lumpur, Malaysia
[2]Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia
[3]Department of Educational Management, Planning and Policy, Faculty of Education,
University of Malaya, 50603 Kuala Lumpur, Malaysia
[4]Network and Communication Security Research Group, ICT and Computational Science Research Cluster,
University of Malaya, 50603 Kuala Lumpur, Malaysia

Abstract: Simple object access protocol or SOAP originally defined as protocol specification for exchanging structured information. SOAP relies on XML for its message format and other application protocols, particularly RPC and HTTP. XML considered as the universal language for data transmission on the Internet, however, end-to-end protection of messages must either be implemented within applications or it can be provided by middleware above the SOAP layer, therefore, SOAP-XML can not provide the level of confidentiality for transferring electronic medical databases. In this paper, we will investigate SOAP protocol structure over XML, the purpose of this paper is identify the possible way towards implementing secure protocol to transfer electronic medical records databases or creating electronic medical records backups over unsecure channels. As a conclusion, SOAP alone can not provide the level of security that medical records databases deserve.

Key words: SOAP, XML, electronic medical records, confidentiality, security

INTRODUCTION

As the number of services and products offered and sold through the Internet grows rapidly, the need to ensure the same level of security as we have in the practical world has become an urgent need in the Internet environment (Ahmed *et al*., 2010; Zaidan *et al*., 2010a-d; Yee and Kiah, 2010). Information security is defined as the field of science that concerns about protecting the information and data from attackers or security threats (Alam *et al*., 2010; Al-Frajat *et al*., 2010; Raad *et al*., 2010). Numbers of method are available to secure data such as encryption methods or to ensure secure access (i.e., authentication) using biometrics (Zaidan *et al*., 2010e-g; Abomhara *et al*., 2010a, b; Qabajeh *et al*., 2009). Data privacy refers to the relationship between technology and the legal right to public expectation of privacy in the collection and sharing of data about one's self (Naji *et al*., 2009; Zaidan *et al*., 2010h-j). Information about health care or electronic medical records classified under high sensitive data that required high secure systems.

According to USA government, 100 billion dollars will be spent on developing electronic medical record for the next 10 years (Alanazi *et al*., 2010a; Yass *et al*., 2010) Services become progressively more important element of national economies and it is crucial to appreciate the distinguishing qualities of services and resulting management implications with specific focus on healthcare services.

Electronic medical records is digital information for a particular patient, this record may be created for each service to this particular patient, such as his/her radiology, pharmacy or laboratory, or as a result of an administrative action such as creating a claims. Moreover, some clinical systems also allow electronic capture of physiological signals such as nursing notes, electrocardiography, orders or physician (Alanazi *et al*., 2010b). Creating backups or transferring electronic medical records database is hard task, not only on

Corresponding Author: Mohamed Shabbir A. Nabi, Department of Computer System and Technology,
Faculty of Computer Science and Information Technology, University of Malaya,
50603 Kuala Lumpur, Malaysia Tel: +6017-3442652

security but on finding a suitable middleware. Unlike securing a single electronic medical record transmission where creating a security solution deals with small data is quite easy comparing with transferring huge database in a secure channel (Alanazi *et al*., 2010b; Hmood *et al*., 2010a-c)

XML is a short form for Extensible Markup Language (XML) and considered as the universal language for data transmission on the Internet. Unlike HTML (which is only for displaying data), XML allows us to define our own tags, XML allows the users to define their own tags written between angled brackets, i.e. a tag in XML opens with symbol and end with symbol.

Example:

```
<note>
<to>John</to>
<from>Patrice</from>
<heading>Reminder</heading>
<body>Don't forget our meeting next week</body>
</note>
```

The example above depicted how XML tags are written. For example <to> and <from> are not defined in any XML standard. However these tags are "created" by the author of the XML document and this is possible because XML language has no predefined tags.

XML documents can be used to represent information independently from the platform and language, and it is universally accepted as the standard technology for information interchange. XML documents can be in a form of a file, database or any other document types and can be created under any languages.

Therefore, XML is used to carry out any kind of data, XML document can be any document defined by Document Type Definition (DTD), DTD defines legal building block of an XML document including:

- Names of element and how and where they can be used
- The order of elements
- Proper nesting and containment of elements
- Elements attribute

XML document can be database file, printer file, other device file (e.g. mobile device file), word processing tool file, editing application file, in-house printing file or browsing file.

- The benefits of using XML over the web are as follows. Simplicity, when we say simplicity that is because Information coded in XML is easy to read and understand, in addition it can be processed easily by computers. Openness, due to XML is a W3C standard. Extensibility that is because there is no fixed set of tags, tags can be created whenever needed. Self-description in traditional databases, data records require schemas set up by the database administrator. XML documents can be stored without such definitions, because they contain XML is a self descriptive that is because metadata is stored in XML in the form of tags and attributes. Can have multiples data types, XML documents can contain any possible data type such as large objects like video, sound, image and etc.
- Distributed data, XML document can contain elements that are distributed over multiple remote servers so that the World Wide Web can be seen as a one huge database

SOAP has not defined any transport protocol; instead SOAP works on existing transport protocols, such as HTTP, SMTP, and MQSeries.

A SOAP method is an HTTP request/response that complies with the SOAP encoding rules A SOAP request could be an HTTP POST or an HTTP GET request.

Example:

```
<SOAP:Envelope xmlns:SOAP=
“http://schemas.xmlsoap.org/soap/envelope/”>
<SOAP:Header>
<!— content of header goes here —>
</SOAP:Header>
<SOAP:Body>
<!— content of body goes here —>
</SOAP:Body>
</SOAP:Envelope>
```

SOAP, stands for Simple Object Access Protocol is a protocol used between applications which has specific format for sending messages on the Internet. SOAP is based on XML hence, SOAP communicates through the Internet independent of the platform and language used.

When an XML documents consists of nested elements which are distributed over multiple remote servers the XML document will look like a huge database over the World Wide Web.

The best way for communication between applications is using HTTP and that is because HTTP is supported by all internet browsers and servers. Hence, SOAP protocol is created to accomplish this task, it uses HTTP and XML for communication between applications, in nutshell, HTTP + XML = SOAP.

SOAP PROTOCOL STRUCTURE

As mentioned earlier, SOAP is a simple XML-based protocol that allowed applications exchange the information over HTTP.

Applications in the Internet communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, however, the best way to communicate between applications is over HTTP, since HTTP is supported by all Internet browsers and servers.

The important of SOAP presented on providing a way to communicate between different applications with different technologies running on different operating systems, and programming languages. SOAP works as follow (Fig. 1):

- A client of SOAP requests for a service. This includes creating an XML document, either explicitly or using Oracle SOAP client API
- Using HTTP or HTTPS the SOAP client sends the XML document to a SOAP server
- Using the SOAP request handler servlet when the web server receives the SOAP message which is an XML document, the server then sends the message to an appropriate server-side application providing the requested service
- In return, a response from the server side service is returned to the SOAP Request Handler Servlet and to the caller using the standard SOAP XML payload format

LITERATURE REVIEW

XML is a great technology as it can deal with any data, any operating system and any programming language. Due to the successes of this technology, XML start growing rapidly. SOAP protocol is XML-based that allowed applications exchange the information over HTTP. W3C start concerning about XML and SOAP security, therefore, they implemented different solutions to secure their data which are as follow:

- **Encryption:** Sensitive data can be encrypted using either symmetric or asymmetric cryptography. Although, the data is sent in the clear; the encrypted part will be opaque and hard to crack. The process and format of the encrypted XML data defines by W3C.
- **Authentication:** SOAP services users' can be authenticated in many ways such as digest authentication and token-based authentication. Token based authentication requires users to supply credentials through a secure channel (i.e. request). SOAP servers respond with an authentication token which can be used for farther requests.
- **Digital signature:** Signature is a technique to ensure the integrity of the data. SOAP messages either partially or the whole documents are first digested. The digest, along with other sensitive data, is then

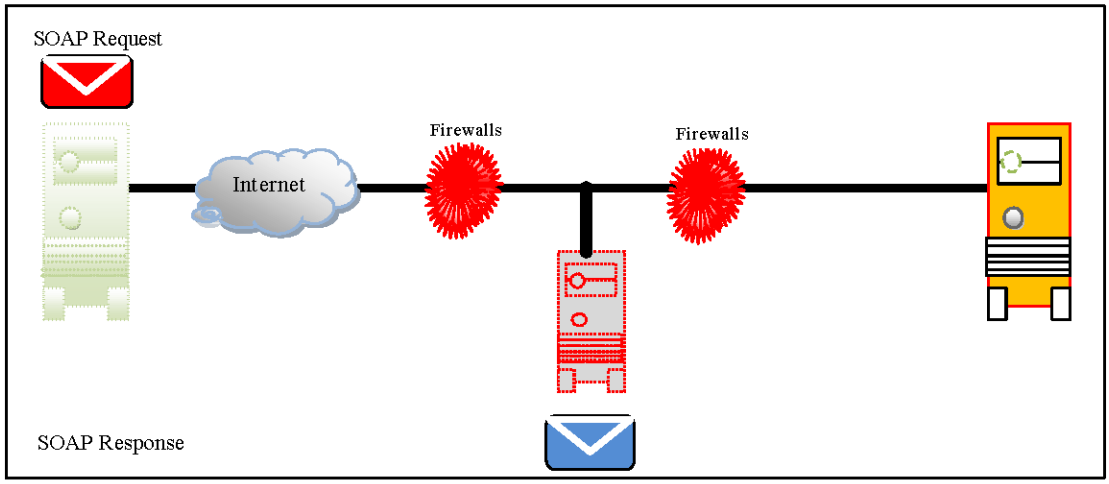

Fig. 1: SOAP request and response

Table 1: Researcher opinion about SOAP

Author	What are the researchers said about SOAP?
(Brose, 2003)	1. Typical medium security mechanisms (firewalls) are effectively overridden once SOAP messages are allowed to cross the domain boundary.
	2. Counection-based security mechanisms such as SSL are not sufficient as they provide only point-to-point protections to messages, but cannot achieve end-to-end security in media where messages traverse multiple intermediaries.
	3. It has been agreed that the de facto standard for Web Services messaging today is SOAP.
	4. The SOAP messaging layer does not offer any security mechanism.
	5. In general SOAP model messages may travel through any number of intermediaries before arriving to the destination, both the sender and the receiver should trust that no intermediary in the communication chaunel violates their security requirements, for example storing and later replaying messages.
	6. Due to the transport protocol layer underneath SOAP is not provided, end-to-end protection of messages must either be implemented within applications or it can be provided by middleware above the SOAP layer
(Davis and Parashar 2002)	1. Because SOAP doesn't specify a transport mechanism, most SOAP RPC implementations use HTTP.
	2. WSDL provides an interface definition language for SOAP. WSDL is not required however the use of WSDL with SOAP is a de facto standard.
	3. SOAP implementations differ in their support for binding to application-defined data types.
	4. It has been found that the encoding and decoding time for SOAP was greater than for protocols such as Java's object serialization.
	5. One of the large sources of inefficiency in SOAP is the use of multiple system calls to send one logical message.
	6. Another source of inefficiency in SOAP is the XML parsing and formatting time.
Chiu, *et al.*, 2002)	1. When two components do not have a shared faster protocol, SOAP over HTTP can still be used as a "fail-over".
	2. SOAP does not allow a user-specified "tolerance" for doubles and floats.
(Nyman *et al.*, 2008)	1. It was argued that dependence on a particular RPC mechanism, in this case SOAP is not good for a generic messaging interface and the interfaces should be defined so that any communications protocol could be used.
(Kohlhoff and Steele, 2003)	1. It has been found that some SOAP implementations suffered from significantly worse performance because of interaction between the Nagle algorithm and the TCP delayed acknowledgment algorithm in the operating systems for the client and server.
	2. The throughput performance of SOAP relative to the other two wire formats is worse for the 100 Mbps network.
	3. The poor performance of SOAP implementations compared to other wire formats cannot be fully explained simply by the fact that SOAP is text–based.
	4. Some results means that a likely cause of the poor performance of SOAP as a wire format is the complexity of the XML
	5. SOAP is poor when compared to binary CDR and the established industry protocol FIX.
	6. Poor performance of SOAP encoders and decoders for use in high performance business applications.
	7. SOAP performance is poor over binary wire formats

digitally signed using the sender's certificate after that encrypted by the receiver's public key. As the signature is encrypted using the receiver's public key, only the receiver can decrypt it then verify the signature and message digest. Signature or hash verification failure gives an evidence for manipulation during the transmission. However, several people have illustrated the weaknesses and drawbacks of SOAP. In Table 1 we reported some researchers' opinion about SOAP.

Even though, the features of SOAP-XML are encouraging; the recent versions of SOAP are not secure. The available security solutions are by hybrid approaches using the existing security mechanisms such as cryptography, digital signatures, tokens and etc.

CONCLUSION

SOAP or Simple object access protocol is specification protocol for exchanging information relies on XML. In this paper, the researcher opinions on SOAP have been reported. In particular, security issues of SOAP and its capabilities on securing high sensitive data, for instance, electronic medical records. As it has mention earlier, end-to-end protection of messages must either be implemented within applications or it can be provided by middleware above the SOAP layer, therefore, SOAP-XML can not provide the level of confidentiality for transferring electronic medical databases. In nutshell, SOAP can not propose alone as a secure protocol for sensitive data such as electronic medical records. For further researches, implementing secure protocol for EMR-database transmission or create remote backups for EMR-database, we need to employ secure and fast cryptography algorithms for instance, AES and Ntru to overcome the weakness of SOAP in term of security and time.

ACKNOWLEDGMENTS

This research has been funded in part from University of Malaya under No. UM.C/625/1. The Authors would like to acknowledge Multimedia University as the Co-funder for this research.

REFERENCE

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan, B.B. Zaidan and O.A. Hamdan, 2010a. Overview: Suitability of using symmetric key to secure multimedia data. J. Applied Sci., 10: 1656-1661.

Abomhara, M., O.O. Khalifa, O. Zakaria, A.A. Zaidan, B.B. Zaidan and A. Rame, 2010b. Video compression techniques: An overview. J. Applied Sci., 10: 1834-1840.

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Alam, G.M., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and H.O. Alanazi, 2010. Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays, 5: 3254-3260.

Alanazi, H.O., H.A. Jalab, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010a. Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4: 2059-2074.

Alanazi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010b. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Brose, G., 2003. Securing web services with SOAP security proxies. Proceedings of the ICWS 03 International Conference on Web Services, pp: 231-234.

Chiu, K., M. Govindaraju and R. Bramley, 2002. Investigating the limits of SOAP performance for scientific computing. Proceedings of the 11th IEEE International Symposium on High Performance Distributed Computing, July 23-26, Edinburgh, Scotland, UK., pp: 246-254.

Davis, D. and M. Parashar, 2002. Latency performance of SOAP implementations. Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, May 22-24, Berlin, pp: 407-412.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010a. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Hmood, A.K., Z.M. Kasirun, H.A. Jalab, G.M. Alam, A.A. Zaidan and B.B. Zaidan, 2010b. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. Int. J. Phys. Sci., 5: 1054-1062.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010c. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Kohlhoff, C. and R. Steele, 2003. Evaluating SOAP for high performance business applications: Real-time trading systems. Proceedings of the WWW 2003, May 20-24, Budapest, Hungary, pp: 1-9.

Naji, A.W., A.A. Zaidan and B.B. Zaidan, 2009. Challenges of hidden data in the unused area two within executable files. J. Comput. Sci., 5: 890-897.

Nyman, J., K. Framling and V. Michel, 2008. Gathering product data from smart products. Proceedings 10th International Conference on Enterprise Information Systems, (EIS'08), Barcelona, pp: 252-257.

Qabajeh, L.K., M.L.M. Kiah and M.M. Qabajeh, 2009. A scalable and secure position-based routing protocol for ad-hoc networks. Malaysian J. Comput. Sci., 22: 99-120.

Raad, M., N.M. Yeasin, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010. Impact of spam advertisement through email: A study to assess the influence of the anti-spam on the email marketing. Afr. J. Bus. Manage., 4: 2362-2367.

Yass, A.A., N.M. Yaseen, B.B. Zaidan and A.A. Zaidan, 2010. SSME architecture design in reserving parking reserving problems in Malaysia. Afr. J. Bus. Manage.

Yee, P.L. and M.L.M. Kiah, 2010. Shoulder surfing resistance using penup event and neighbouring connectivity manipulation. Malaysian J. Comput. Sci., 23: 121-140.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Fraja and H.A. Jalab, 2010a. Investigate the capability of applying hidden data in text file: An overview. J. Applied Sci., 10: 1916-1922.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010b. An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Applied Sci., 10: 2161-2167.

Zaidan, A.A., B.B. Zaidan, H.O. Alanazi, A. Gani, O. Zakaria and G.M. Alam, 2010c. Novel approach for high (secure and rate) data hidden within triplex space for non multimedia file. Sci. Res. Essays, 5: 1965-1977.

Zaidan, A.A., B.B. Zaidan, A.Y. Taqa, K.M.S. Mustafa, G.M. Alam and H.A. Jalab, 2010d. Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci., 5: 1992-2000.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010e. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zaidan, B.B., A.A. Zaidan, A. Taqa, G.M. Alam, M.L.M. Kiah and H.A. Jalab, 2010f. StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int. J. Phys. Sci., 5: 1796-1806.

Zaidan, A.A., H.A. Karim, N.N. Ahmed, G.M. Alam and B.B. Zaidan, 2010g. A new hybrid module for skin detector using fuzzy inference system structure and explicit rules. Int. J. Phys. Sci., (In Press).

Zaidan, A.A., N.N. Ahmed, H.A. Karim, G.M. Alam and B.B. Zaidan, 2010h. Increase reliability for skin detector using backprobgation neural network and heuristic rules based on YCbCr. Sci. Res. Essays, 5: 2931-2946.

Zaidan, A.A., H.A. Karim, N.N. Ahmed, G.M. Alam and B.B. Zaidan, 2010i. A novel hybrid module of skin detector using grouping histogram technique for bayesian method and segment skin adjacent-nested technique for neural network. Int. J. Phys. Sci., (In Press).

Zaidan, A.A., N.N. Ahmed, H.A. Karim, G.M. Alam and B.B. Zaidan, 2010j. Spam influence on the business and economy: theoretical and experimental study for textual anti-spam filtering using mature document processing and naïve bayesian classifier. Afr. J. Bus. Manage., (In Press).