International Journal of Scientific Research and Management (IJSRM)
||Volume||09||Issue||05||Pages||EC-2021-597-603||2021||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v9i05.ec02

Cryptographic protocol to data exchange in hostile machines

[1]Alex Fabianne de Paulo, [2]Ilmério Reis da Silva, [2]João Nunes de Souza

[1] School of Information and Communication, Federal University of Goiás, Brazil.
[2] School of Computer Science, Federal University of Uberlândia, Brazil.

Abstract
The technology continuous advancement, especially of Internet, has allowed the evolution of the computers usage from a situation that it was used just for simple and isolated tasks to the current global integration level, in which it wants to join the diverse points of generation and use of the information inside and outside of an institution. This has created several possibilities to improve the service quality and information access. On the other hand, new challenges like information heterogeneity and secure appear. This paper presents a new XML-based cryptographic protocol to access and manipulate encrypted data in machines that are susceptible to intruder's attacks. Following the RSA algorithm, this new protocol defines rules in which the encrypted data are handled independent from the user keys and without access of intruders in the others encryption keys and plain text.

Keywords: Cryptography, database security, protocol, XML, secure data exchange

1. Introduction

The technology continuous advancement, especially of Internet, has allowed the evolution of the computers usage from a situation that it was used just for simple and isolated tasks to the current global integration level, in which it wants to join the diverse points of generation and use of the information inside and outside of an institution. This has created several possibilities to improve the service quality and information access. On the other hand, new challenges like information heterogeneity and secure appear.

A large amount of heterogeneity data is available on Intranets and Internet on a non-structuralized or half-structuralized way. These data need to be accessible in a uniform and integrated way for both final users and software application layers. Because of HTML (HyperText Markup Language) limitations [6], these data are presented on an inadequate form, without clarity in separation between document structure and content. Consequently, the HTML markup is inadequate since the objective is to understand the data semantics. In order to surpass the heterogeneity data problem, a great effort was made to provide a cautious markup technique that does not lose the HTML formatting and distribution potentialities. The main result of this effort for standardization is eXtensible Markup Language (XML), a solution for better representation and data exchange in the Internet specified by IETF/W3C XML Working Group [5].

In this context, the use of security mechanisms is essential to guarantee security, mainly regarding to confidentiality and authenticity. The data necessity of privacy and authenticity is evident under the focus of a commercial transaction. When the transaction involves different users, different parts of the system need different types of authentication [1]. Considering an application that makes available critical information contained in a laboratory exam result. The simplicity and interoperability of XML language allow getting these data in different kinds of devices such as palmtops, mobile telephones or desktops, and manipulated them in different applications. But the information secrecy is crucial to guarantee that the exam result is not going to be accessed or violated for someone else. The union of XML standard and security mechanisms makes the data exchange through the Internet a more efficient and secure task.

There are two aspects that need to be solved in this context. First, the user shares its certificate with a server in a previous time. Later, when the user queries this server to exchange data but its certificate is expired, it can't be successful in its query. Then, the user needs to replace your old certificate for a new one. Second, within the user replace its certificate, the encrypted data needs to be decrypted and after it is re-encrypted using the new user key. In this moment, an intruder can get access to the server and monitor the server main memory during this re-encrypted processing. Then, it can discover all information about that user such as plain text and keys. Notice that this problem can't be solved by traditional security techniques used on networks and database like firewalls and cryptographic algorithms. It is necessary to create a secure protocol, which allow the user update its certificate without exposing the plain text and keys. For this, it is necessary that the data to be stored in an encrypted way on second memory and manipulated on main memory without decrypt it. The data can be visible to anyone but only understandable to authorized user [13].

This paper presents a new XML-based cryptography protocol to access and manipulate encrypted data in machines susceptible to intruder's attacks. This new protocol defines rules in which the encrypted data are handled independent from the user public key and without access of intruders in the others encryption keys and plain text. The data system security is equivalent to the cryptographic system it utilizes. In this case, the cryptographic system is based on RSA scheme. The main contribution of this paper is a cryptographic protocol, which allows exchanging the user key for another one in an encrypted data without requires decrypting it.

2. Materials and Methods

2.1. Related works

An authentication protocol such as Kerberos gets data security during its transmission but consider the main memories of user and server protected against intruders. Other secure protocols guarantee confidentiality, integrity and authenticity but providing this security on the transport layer, such as IPSec (Internet Protocol Security) or SSL (Secure Sockets Layer) [11]. In our protocol, the main memories of the machines are vulnerable to intruder's attacks. In order to avoid this, our protocol proposes a way to access and manipulate some encrypted data with no need to decrypt any data in the main memories of these hostile machines.

A multi-user protocol and data exchange protocol able to manipulate stored encrypted data with no need to decipher is proposed in [14]. This protocol is based on elliptic curves cryptography (ECC) [11, 15]. Our protocol is able to re-encrypt the data without decrypt it and expose the keys and the plain text. Instead of using ECC, a cryptographic protocol based on public key is used, more specifically, on the RSA scheme [11,16]. Although the ECC system has a better performance than RSA, we used the RSA scheme because it is based on exponential operations, which is essential to update the user keys without need to decrypt the data.

2.2. Security Requirements

Several applications need security, especially to support the following aspects: (i) confidentiality to guarantee that the data contained in a document is not going to be accessed by non-authorized parts; (ii) authenticity to assure that the document proves a correctly identified origin, with the guarantee that the identity is not false; (iii) integrity to detect if some data contained in the document was modified; (iv) non-repudiation to guarantee that the sender does not deny the sending nor the receiver denies the act of receiving the document.

In order to support the security requirements as described in the previously, we choose XML encryption/signature to guarantees the data confidentiality, authenticity and non-repudiation in the application layer. Specifically in case which the data needs to be protected before and after been transmitted, the use of cryptography assures the data security through the XML encryption [2] and digital signature [4]. The main motivation for the use of cryptography based on XML syntax instead of using a binary or text based syntax is the necessity to have the encrypted or signed data as structures that can be created, manipulated and analyzed with XML tools [1].

2.3. The RSA Scheme

The RSA scheme is based on numbers theory and use an expression with exponentials [17, 18]. The RSA key generation, encryption and decryption process are in the following way:

1. Choose two prime numbers p, q. The values of p, q are private;
2. Calculate $n = p \times q$. The value of n is public;
3. Calculate $\phi(n) = (p-1)(q-1)$ where $\phi(n)$ is the Euler totient function, which is the number of positive integers less than n and relatively prime to n;
4. Select a public integer e such as $\gcd(\phi(n), e)=1$ and $1 < e < \phi(n)$;
5. Calculate $d = e^{-1} \bmod \phi(n)$ where d is private;
6. Then it is possible determine the public and private keys, KU and KR, which KU = $\{e, n\}$ and KR = $\{d, n\}$.

The encryption and decryption process occurs as following for a plain text M and ciphertext C (equation 1):

$$C = M^e \bmod n \qquad (1)$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

But three requirements must be met for this algorithm to satisfy the public-key encryption as following:

- It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M < n$;
- It is relatively easy to calculate M^e and C^d for all values of $M < n$;
- It is infeasible to determine d given e and n. In order to attend this last requirement, it essentially that p and q must be large prime numbers.

3. Results and Discussion

3.1. Cryptographic protocol scheme: case study

The continuous technological advances have provided a revolution in the medicine. The use of computer in the hospital developed to a situation where the health professionals depend on the computer to get diagnosis that is more precise. Furthermore, the number of medical institutions and professionals who try to offer a better attendance to the users is increasing, as much in time as much in cost. In this direction, the use of computer science resources is an essential stage. The worldwide trend points in direction to the patient clinical record digitalization through the patient electronic record. But, for many countries, the absent of an exclusive number that identifies to all the citizens since its birth, the lack of government support and the absence of a legislation that gives legal validity to the electronic record are some of the factors that make it difficult the evolution of the medical sector to the creation of the patient electronic record [9].

```
<Exam xmlns='http://www.medclin.com/examresult'>
   <Patient_Data>
        <Cod>589476-02</Cod>
        <ID>John Calvet</ID>
   </Patient_Data>
 <Result>...</Result>
</Exam>
```

Figure 1: XML data structure of an exam result

Searching continuous evolution, but still distant of the electronic record idea, there are several initiatives to make the laboratory exam results available on the Web. This process contributes mainly in accessibility and agility of exam result for the interested people either it, medical or patient. But some kinds of exams are critical and decisive results for the patient life. Ahead of this, this paper presents a new secure protocol that define rules to exchange exam results using XML standard and allows which data to be manipulated without need to decrypt them. The figure 1 shows the data exam result after be converted to XML structure.

3.2. Notation

Some important notes are pointed on this section. As first notation is the syntax used in the protocols. The logical propositional symbols $\vee$, $\wedge$ (or, and) are used in some flows of the protocols. The characters "C" and "D" express respectively encryption and decryption functions. The response value "ex" refers to the plain text of exam result and "exXML" indicates the plain text of exam result converted to XML standard. Other two kinds of response values are allowed: "N" represents a null value used to indicate that the data is invalid or not found, and "Cod" value that refers to exam identification code. The public and private keys are represented in KU and KR. These keys are different for user and laboratory following the "U" and "L" indexes.

Second important note, all operations over XML data, like canonicalization, encryption or digital signature following the syntax specified on IETF/W3C Working Group [2, 4, 7]. Third, the way in which the data of the exam result will be encrypted is another point. In both protocols will be encrypted only the element <Result>, leaving the user identification and the exam identification code opened. Fourth, due to the portability and interoperability characteristics of XML language in both protocols, the user can access the laboratory servers through different devices like palmtops, mobile telephones or desktop computers. Last, the use of public key certificates [11], will allow that the user and laboratory can exchange keys in trustworthy way without having to directly interact with a public key certificate authority. The certificates are previously gotten by each system entity (user and laboratory) together to a certificate authority.

The authority provides the certificate in the following form (equation 2):

$$C = E_{KRAUT} [T, ID, KU] \quad (2)$$

which, C_E is the solicitant entity certificate, KRAUT is the certificate authority private key, T defines the validity of the certificate, ID is solicitant entity identification (name or code) and KU is the solicitant entity public key. C is obtained through the encryption of [T, ID, KU] with the private key KR_{AUT} of certificate authority.

Thus, C can be passed to any other entity, which could read and verify the certificate, decrypting C with the public key KU_{AUT} of the certificate authority and getting [T, ID, KU]. This process follows this equation 3:

$$D_{KUAUT} [C] = D_{KUAUT} [E_{KRAUT} [T, ID, KU]] = [T, ID, KU] \quad (3)$$

Because the certificate is readable only using the authority's public key, this verifies that the certificate came from the certificate authority.

3.3. Data encrypted storage

In the moment that a user goes to laboratory to do an exam, it leaves there its certificate C_U. In an off-line way, without any possibility to espionage, the exam results in a plain text form are input on the laboratory back-end server. But, before storing it in a database, the back-end server converts the exam results plain text ex to a XML version (ex$\rightarrow$exXML). Next, the back-end server starts the process to encrypt exXML. Thus, the back-end server, gets two prime numbers p, q and calculates n and $\phi(n)$. To store the exXML on an encrypted form, the back-end server calculate Z and X as following (equations 4 and 5):

$$Z = (exXML)^{KUL} \bmod n \quad (4)$$

$$X = KU_U \,.\, KR_L \bmod \phi(n) \quad (5)$$

where, KU_L is the laboratory's public key, KU_U is the user public key and KR_L is the laboratory's private key. See the table 1 which the data, now encrypted, will be stored on the database represented by the two tuples:

- Tuple 1: represented by user identification name (ID) and keys composition X;
- Tuple 2: composed by user identification name (ID), exam identification code (Cod) and the encrypted data represented by Z.

Tuple 1

ID	X
...	...
...	...
...	...

Tuple 2

ID	Cod	Z
...	...	...
...	...	...
...	...	...

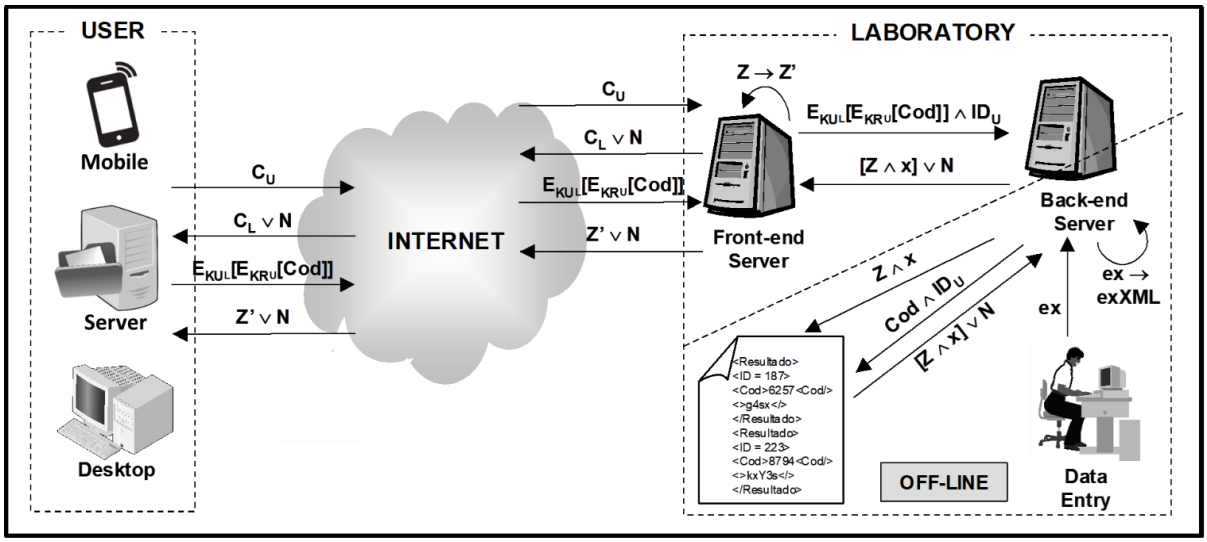
Table 1: Representation of encrypted data on database

In two tuples, the secrecy data contained in Z and X are encrypted. The user identification name (ID) and the exam identification code (Cod) are stored in non-encrypted. Once the data is encrypted, it stored on the database and available just encrypts form. Although Z is public, it is safety because Z was encrypted using the laboratory public key. Therefore, just the laboratory can access and decrypts Z using its KR_L. Moreover, X and KU_U are public but it is infeasible to discover KR_L over these public values because $\phi(n)$ is a large number and by RSA scheme this reverse calculate is infeasible.

3.4. Data exchange scheme

Suppose a user, either it patient, responsible doctor or another person assigned by the patient, send to laboratory a public key certificate (CU) to get its respective exam result. In the laboratory front-end server, the user certificate (CU) is decrypted with the authority public key (KUAUT), getting the user identification (IDU), its public key (KUU) and the certificate validity (TU). The front-end server returns to user the laboratory certificate (CL) or a null value message (N), indicating that the user certificate expired and the user needs to replace the old certificate for new one. It can be seen in figure 2 as indicated by [CL $\vee$ N].

Figure 2: Protocol scheme to secure data exchange



In case that the user does not receive the null value message, it gets from C_L the laboratory public key (KU_L). At this moment, the user must send to laboratory the exam identification code (Cod). For this, the user signs Cod with its private key (KR_U), later encrypted it with the laboratory public key (KU_L) and sends the encrypted Cod to the laboratory front-end server, as indicated in the figure 2 by $E_{KUL}[E_{KRU}[Cod]]$.

In case that the user does not receive the null value message, it gets from C_L the laboratory public key (KU_L). At this moment, the user must send to laboratory the exam identification code (Cod). For this, the user signs Cod with its private key (KR_U), later encrypted it with the laboratory public key (KU_L) and sends the encrypted Cod to the laboratory front-end server, as indicated in the figure 2 by $E_{KUL}[E_{KRU}[Cod]]$.

To get the exam identification code (Cod), the front-end server forwards $E_{KUL}[E_{KRU}[Cod]]$ and ID_U to back-end server that deciphers it using laboratory private key (KR_L) and verify the user signature using user public key (KU_U). Known Cod and ID_U, the back-end server queries to the encrypted database of exam results to obtain the exam result of corresponding Cod and ID_U. It is shown in the flow [Cod $\wedge$ ID_U] of figure 2. If the exam identification code or the user identification is not found, the back-end forwards a null value message (N) to front-end server that forwards N to user. But in case that a corresponding result to Cod and ID_U is found on the database, the back-end server receive Z, X and forwards them to front-end server. The front-end server gets Z and X, and executes the follow calculation in its main memory (equation 6):

$$\begin{aligned} Z' &= Z^X \bmod n \\ Z' &= (\text{exXML})^{KUL.KUU.KRL} \bmod n \\ Z' &= (\text{exXML})^{KUU} \bmod n \end{aligned} \qquad (6)$$

where Z' is Z raised X module *n* used to obtain the exXML raised KU_U module *n*. This calculation allow the user decrypts Z' using its private key and obtain exXML plain text. Note that it wasn't showed exXML plain text or some used keys any time.

In the situation, which the user receives, a null value message indicating certificate expiration, the user can replace the expired certificate for a new and valid one. For this, the user sends to laboratory its new certificate C_U'. The laboratory front-end server validate C_U' and forwards C_U' to back-end server. In off-line way, the back-end server recalculates only X. Note that Z was not recalculated Z. It is represented better performance than calculates all data encrypted, besides not expose the plain text and keys on the server's main memory. Then, in another moment, the user should reconnect to laboratory to get its exam result encrypted and updated with its new user certificate.

4. Conclusions

This paper presented a new XML-based cryptographic protocol to access and manipulate encrypted data in machines which are susceptible to intruder's attacks without need to decrypting. In the proposed context, all stored data is encrypted. Besides the machines are hostile, it is infeasible for an intruder discovers the keys and plain texts because the data is stored in an encrypted way. In cases that are necessary replace the expired user certificate; just part of keys is manipulated. In this situation, the operation is done off-line. This protocol dispenses any external security device like firewalls. Based on RSA scheme, the security of this protocol is equivalent to security of RSA.

As future works, the goal is to improve this protocol using the concept of atomic proxy function [12] to solve the problem of user certificate expiration. In addition, it is planned to this protocol can be implemented and several tests can be done to measure its efficiency.

5. Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

6. References

[1] Eastlake III, D. E., Niles, K., Secure XML: The New Syntax for Signatures and Encryption, Addison-Wesley, Boston, 2002.

[2] W3C, *XML Encryption Syntax and Processing*, http://www.w3.org/TR/xmlenc-core/, December 10, 2017.

[3] W3C, *Decryption Transform for XML Signature*, http://www.w3.org/TR/xmlenc-decrypt, December 10, 2017.

[4] W3C, *XML-Signature Syntax and Processing*, http://www.w3.org/TR/xmldsig-core/, February 12, 2018.

[5] W3C, *Extensible Markup Language (XML) 1.0 (Second Edition)*, http://www.w3.org/TR/REC-xml, February 4, 2018.

[6] W3C, *HTML 4.01 Specification*, http://www.w3.org/TR/REC-html40, December 24, 2017.

[7] W3C, *Canonical XML Version 1.0*, http://www.w3.org/TR/2001/REC-xml-c14n-20010315, March 15, 2018.

[8] Johanston, H., *Sistemas de Informação Hospitalar: Presente e Futuro*, Revista Informédica, in http://www.epub.org.br/informed, São Paulo, v.1, n.2, 1993.

[9] E-Health Latin America, *Há um Futuro Promissor na História Clínica Eletrônica*, Bibliomed, in http://www.bibliomed.com.br, November 2000.

[10] Kohnfelder, L., *Towards a Practical Public-Key Cryptosystem*, Bachalor's Thesis, M.I.T., May 1978.

[11] Stallings, W., *Cryptography and Network Security*, Principles and Practice, Prentice Hall, New Jersey, 1999.

[12] Blaze M., Strauss, M., *Atomic Proxy Cryptography*, AT&T Labs-Research, February 1998.

[13] Castano, S., Fugini, M., Martella, G., Samarati, P., *Database Security*, Addison-Weslwy, 3rd edition, 2000.

[14] Souza, J. N., Moreira, M. A. R., Silva, I. R., *A Multi-User Key and Data Exchange Protocol to Manage a Secure Database*, XVII Simpósio Brasileiro de Banco de Dados, 14-16 October 2002, Gramado Rio Grande do Sul, Brasil, Anais/Proceedings.

[15] Blake, I., Seroussi, G., Smart, N., *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[16] Stinson, D. R., *Cryptography, Theory and Practice*, CRC Press, 1995.

[17] Coutinho, S. C., *The Mathematics of Ciphers: Number Theory and RSA Cryptography*, A K Peters, 1998.

[18] Koblitz, N., *Algebraic Aspects of Cryptography*, Springer, 1999.