XML Data Security

Basavaraj G. Shirur

Abstract---The extensible Markup Language (XML) has been attracted much attention for expressing much of the Web’s content and data exchange. However, the use of the internet and multimedia technology these days has encouraged the intruders to copy the contents and illegal use of the data which is available on the internet or any other resources. Therefore the integrity protection of XML documents is becoming highly important. In this paper, we present a brief overview of XML related technologies and data security. Moreover, we introduce an experimental example for encrypting XML data based on chaos method.

Keywords---XML, Data security, Encryption.

I. INTRODUCTION

The recent growth of the Internet and invention of the XML technology data format has created the need for businesses to exchange information, and to interoperate in a uniform way. XML has rapidly become a de facto standard for document and data exchange. The extent of its growth is indicated by the growing research in several of the XML and its applications; a series of standards has grown up around it, many of which were defined by the World Wide Web Consortium (W3C) [1]. An XML document is a stream of characters, which can be encrypted just like any other document.

Any encryption program that can encrypt any document can encrypt an XML file. The problem is that doing so restricts the ability to make use of the full power of XML. Encrypting an XML file will result in a binary stream which is not in the XML format, therefore it needs specialized processing to read and understand. For this purpose, for encrypting an XML file should result into a new XML files.

The first standard that the W3C produced in the XML cryptography space was XML Signature and the second major XML security specification from the W3C is XML [2]. Watermarking is the process of embedding the information into another object or signal. Its applications mainly used for copyright-protection, through which the owner can prove his ownership or trace any reproduction of the original data. For more effective, the watermark should have the characteristics such as Perceptual Transparency, Robustness, Universality, Capacity, Payload, and Unambiguousness. The rest of the paper is organized as follows. The next section describes XML and related technologies, after that we introduce a brief survey of XML Data Security, XML watermarking techniques, and we present an example for experimental results and conclusions.

II. LITERATURE SURVEY

A. XML Data Security

Without any defenses, it is obvious that there are several security threats, and to get around the potential threats, three general security functions: Authentication, Message Integrity and Confidentiality are needed. For this reason we discuss about encryption, signature and key exchange method. XML Encryption is an encryption technology that provides end-to-end security for applications that require secure transmission of XML data. It solves the security problems such as confidentiality, integrity and authentication.

XML Encryption standards provide mechanisms for the strengths of XML in applications with cryptographic requirements [3]. For the XML Encryption standards provide two complementary capabilities. Firstly, the XML document, much of the mark-up structure can be modified in ways that do not change the actual meaning of the data. The XML Signature standard provides a means of ensuring changes so that it will not impact on the meaning of a data. Secondly, the standards provide powerful and flexible signature and encryption mechanisms that build on the native abilities of XML. XML Encryption also provides advanced features such as: Partial encryption: encrypts XML data within specific tags, Multiple encryptions: encrypts XML data multiple times using different keys, Complex encryption: encrypt particular portion of the XML tags according to the designation of the recipient.

B. XML Signature

XML Signature is an electronic signature technology which is defined to be used in XML data transmission. XML Signature provides a standard for signing an XML document and representing a digital signature in an XML format. XML Signature specification [4], defines electronic signature formats using XML, the creation of electronic signature and rules for the verification process. It solves security problems such as authentication, integrity and non-repudiation. Further to this, XML Signature provides advanced benefits such as partial signature; allows only data contained in specific tags to be signed in the XML document and multiple signature; enables multiple electronic signatures to be included in the XML document.

There are various type of transforms in XML signature. They are simply algorithms that are applied to an XML document and which result in a new XML document. These transforms such as: Canonicalization: XML Signatures are complemented by Canonical XML, which specifies an
XML Encryption generally has presented fewer problems than XML Signature. However, one unfortunate effect is that the presence of encrypted data in a message is automatically schema invalid, thus preventing schema checking of the remainder of the XML.

Some standards have defined schemas which may include encrypted data, but it would be better to deal with this in a more comprehensive way. As is the case with Signature, the flexibility of XML Encryption has led to the discovery of new types of security threats.

In some cases, the use of encryption has interacted with other protocols to create new threats. [McIntosh] In other case, the interactions between XML Encryption and XML Signature has been the source of new threats.

We consider a case when a user wishing to place an order with an online retailer. The order will include the user’s identification, identification of the ordered goods, and payment information (such as a credit card). The user will want to keep private, i.e., encrypt, the payment information. The retailer wishes to authenticate the user to make sure no fraudulent orders are placed, which requires a digital signature. Authenticating the retailer to the user is better handled at the messaging protocol level, and not at the message level.

The following XML document is used as original data for XML encryption.

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<PaymentInfo>
  <Name>John Smith</Name>
  <CreditCard>
    <Issuer>Example Bank</Issuer>
    <Number>4019 2445 0277 5567</Number>
    <Expiration>04/02/2008</Expiration>
  </CreditCard>
</PaymentInfo>
```

### C. XML Key Managements

The XML Key Management Specification (XKMS) provides an interface between XML applications and a Public Key Infrastructure (PKI) and also it specifies protocols for distributing and registering public keys [6]. This specification eliminates the complex PKI application logic implementation at the client side and allocates trust processing decisions to separate trust processors. XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS) are two major subparts of the XKMS [7]. Recently, XML can be used to define languages for expressing protection requirements for any kind of data/resources [14]-[15].

### III. XML Signature Issues

This section describes issues relating to the use of XML Signature.

- a) No Completely Satisfactory Canonicalization Algorithm
- b) Spurious Validation Errors
- c) No Satisfactory Way to Reference Arbitrary Inserted Contend
- d) Adding or Removing an Id Can Break Signatures
- e) Id Attributes Can Create Security Threats

### IV. XML Data Security

#### A. XML Encryption

XML Encryption has been the source of new threats. [McIntosh] In other case, the interactions between XML Encryption and XML Signature has been the source of new threats.

By encrypting the entire Credit Card element from its start to end tags, the identity of the element itself is hidden.

#### C. Decryption of XML Document

For decryption of the XML document, also we required the exact value of the initial values and threshold. The process of decryption consists of the following steps:

1. Read the encrypted XML file in the binary form.
2. Generate the pseudorandom sequence using initial condition.
3. Generate the binary pseudo-random sequence using the threshold.
4. X-or the binary pseudorandom sequence and encrypted portion.

Select the for decryption initial value as \( \mu = 3.57 \), \( x_0 = 0.7 \) and \( t=5 \), then we are able to recover the exact form of the encrypted XML file.

We consider a case when a user wishing to place an order with an online retailer. The order will include the user’s identification, identification of the ordered goods, and payment information (such as a credit card). The user will want to keep private, i.e., encrypt, the payment information. The retailer wishes to authenticate the user to make sure no fraudulent orders are placed, which requires a digital signature. Authenticating the retailer to the user is better handled at the messaging protocol level, and not at the message level.

The following XML document is used as original data for XML encryption.

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<PaymentInfo>
  <Name>John Smith</Name>
  <CreditCard>
    <Issuer>Example Bank</Issuer>
    <Number>4019 2445 0277 5567</Number>
    <Expiration>04/02/2008</Expiration>
  </CreditCard>
</PaymentInfo>
```
decryption. If we select $\mu = 3.57$, $x_0 = 0.7001$ and $t = 5$, then the decrypted portion as:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<PaymentInfo>
   <Name>John Smgsf</Name>
   <CreditC_qb/>
</PaymentInfo>
```

The decrypted xml is not same as original if we take different initial value.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we have briefly discussed the XML data security. Also, we have introduced an experimental example for XML data encryption based on the chaos technique. In the future, we plan to investigate the hiding the data in the four level wavelet transform & piecewise linear chaotic map for making it more robust against various types of the attacks.

REFERENCES


Basavaraj G. Shirur Studying Computer science in SKSVMACET-LAXMESHWAR, India. (E-mail:Basavaraj10008@gmail.com)