A Security Acceleration Using XML Signcryption Scheme in Mobile Grid Web Services

Namje Park[1], Kiyoung Moon[1], Kyoil Chung[1], Dongho Won[2], and Yuliang Zheng[3]

[1] Information Security Research Division, ETRI,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{namejepark,kymoon,kyoil}@etri.re.kr
[2] School of Information and Communication Engineering, Sungkyunkwan University,
300 Chunchun-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea
dhwon@dosan.skku.ac.kr
[3] The University of North Carolina at Charlotte,
9201 University City Boulevard, Charlotte, NC 28223-0001, USA
yzheng@uncc.edu

Abstract. Today's grid architecture encompasses a far greater breadth of applications than the traditional grid, which focused on distributed applications processing large amounts of data. Newer grid applications are more data-centric and more focused on distributed services. As these trends, mobile internet and the grid, are likely to find each other the resource constraints that wireless devices pose today affect the level of interoperability between them. The goal of this paper is to investigate how well the most limited wireless devices can make the use of grid security services. This paper describes a novel security approach on fast mobile grid services based on current mobile web services platform environment using XML signcryption mechanism.

1 Introduction

Besides mobile internet the traditional Internet computing is experiencing a conceptual shift from client-server model to grid and Peer-to-Peer (P2P) computing models. As these trends, mobile internet and the grid, are likely to find each other the resource constraints that wireless devices pose today affect the level of interoperability between them. As these key trends, mobile Internet and the grid, are likely to find each other the resource constraints that wireless devices pose today affect the level of interoperability between them [1].

Furthermore, open mobile grid service infrastructure will extend use of the grid technology or services up to business area using web services technology. Therefore differential resource access is a necessary operation for users to share their resources securely and willingly. Therefore, this paper describes a novel security approach on fast mobile grid services based on current mobile web services platform environment using XML signcryption mechanism.

2 The Performance Problem and XML Signcryption

XML-based messaging is at the heart of the current grid based on web services technology. XML's self-describing nature has significant advantages, but they come at the

D. Lowe and M. Gaedke (Eds.): ICWE 2005, LNCS 3579, pp. 191–196, 2005.

price of bandwidth and performance. XML-based messages are larger and require more processing than existing protocols such as RMI, RMI/IIOP or CORBA/IIOP: data is represented inefficiently, and binding requires more computation. For example, an RMI service can perform an order of magnitude faster than an equivalent web service-based grid. Use of HTTP as the transport for Web services messages is not a significant factor when compared to the binding of XML to programmatic objects [9].

Increased bandwidth usage affects both wired and wireless networks. Often the latter, e.g. mobile telephone network, have bandwidth restrictions allotted for communication by a network device. In addition, larger messages increase the possibility of retransmission since the smaller is the message, the less likely it will be corrupted in the air. Increased processing requirements affect network devices communicating using both types of networks (wired and wireless). A server may not be able to handle the throughput the 'network' demands of it. Mobile phone battery life may be reduced as a device uses more memory, performs more processing and spends more time transmitting information. As the scale of web services usage increases, these problems are likely to be exacerbated. Fast grid services attempts to solve these problems by defining binary-based messages that consume less bandwidth and are faster and require less memory to be processed. The price for this is loss of self-description. Fast grid service is not an attempt to replace XML-based messaging. It is designed to be an alternative that can be used when performance is an issue.

XML signcryption structure and schema has been proposed. Shown below is the XML signcryption XML document. The root element XML signcryption is the fundamental element of the XML documents. Within the root element are contained various other elements such as signed info and the signcryptionvalue, Rvalue and Svalue [6,7].

```
<?xml version="1.0" encoding="UTF-8" ?>
< XML_Signcryption >
  <SignedInfo>
    <CanonicalizationMethod Algorithm />
      <SignatureMethod Algorithm />
      <EncryptionMethod Algorithm />
      <Reference URI>
        <DigestMethod1 Algorithm />
        <DigestMethod2 Algorithm />
        <DigestValue />
      </Reference URI>
  </SignedInfo>
  <SigncryptionValue></SigncryptionValue>
  <Rvalue></RValue>
  <Svalue></Svalue>
</ XML_Signcryption>
```

Fig. 1. Proposed XML Signcryption Schema

The signedInfo element contains the information about the signcryption methodology used. It described about the implementation details about signcryption. Within the signed info element there are other elements such as CanonicalizationMethod Algorithm, SignatureMethod Algorithm, EncryptionMethod Algorithm and Reference URI.

The CanonicalizationMethod indicates the method that is used for canonicalization. The canonical method allows the use of different characters in the XML docu-

ment. For example, if there are white spaces in the xml document, these are removed because of the XML canonicalization method used. The signatureMethod element indicates the signature element used in the signcryption process. EncryptionMethod is the encryption method that is used in the signcryption process. In our example, the algorithm used is DES. The element Reference indicates the link of the file that is being signcrypted. It contains the path of the file that is being signcrypted. The reference URI also contains the different Hashing algorithms that are being used in the signcryption process. In our implementation, we are using MD5 and SHA1.

As indicated in sections above, the result of signcryption are three values, namely c, r and s. these three values are required by the system to create the plain text from these messages. When signcryption is performed on a data, the output is a signcryption value. Signcryption requires different digest functions. The description of the hash functions and also the different parameters required for encryption. The encryption method that is used for signcryption is also shown in the XML document. This information is also shown in the Canonicalization method is used to embed a document in another document. Using Xpath filtering, an appropriate file is opened so that the file is opened using the application specified.

```
<element name="XML_Signcryption" type="SigncryptionType"/>
  <complexType name="SigncryptionType">
   <sequence>
    <element ref="SignedInfo"/>
        <element ref="SignatuereMethod"/>
        <element ref="EncrptionMethod" />
        <element ref="Reference" minOccurs="0"/>
   </sequence>
        <attribute name="Id" type="ID" use="optional"/>
        <attribute name="MimeType" type="MIME" use="optional"/>
        <attribute name="Mode" type="MODE" use="required"/>
        <attribute name="Type" type="TYPE" use="required"/>
        <attribute name="Encoding" type="CODING" use="optional"/>
  </complexType>
 </element>
```

Fig. 2. Signcryption Schema

XML signcryption schema is shown above. The schema is required to validate the received XML message for its integrity. A part of the XML signcryption module is to create a technique where in badly formed XML documents need to be removed. Survey shows that a lot of attacks on XML servers are due to the fact that the XML documents created are not properly formed. The hardware-based solutions perform this additional task. The software-based module also needs to check the validity of the schema before the document is passed onto the next stages for verification.

The schema defines the various attributes and the elements that are required in a XML document. These attributes declare the feature of the XML document. The Id the element possesses and Multipurpose Internet Mail Extensions (MIME) so as to allow non-textual message to be passed can be incorporated into the XML document. The mode in which the signcryption has occurred, Type specifies a built-in data type.

The XML signcryption schema and is being used with Java Crypto Extensions and SAX parser to create a XML signcryption module. As the signcryption algorithm is faster compared to other signature algorithms, because of its reduced computation, the system is faster. This system introduces faster processing and also provides an

additional feature of encryption along with the signature. Hence, the XML signcryption not only performs the integrity of the XML document, but also performs the confidentiality of the system. This additional facility is provided to the system with faster execution time.

The proposed XML signcryption test environment, as shown in figure 4, an XML document is parsed and schema is validated using SAX parser. After the XML document is validated, the information is passed to signcryption module. The signcryption components can verify/generate the signature for an XML document.

3 Middleware Framework for Secure Mobile Grid Service

A security framework using grid middleware for mobile grid services is as follows figure 3. Web services can be used to provide mobile security solutions by standardizing and integrating leading security solutions using XML messaging. XML messaging is referred to as the leading choice for a wireless communication protocol and there are security protocols for mobile applications based upon it. Among them are the follows. SAML (Security Assertions Markup Language) is a protocol to transport authentication and authorization information in an XML message. It could be used to provide single sign on web services. XML signatures define how to digitally sign part or all of an XML document to guarantee data integrity. The public key distributed with XML signatures can be wrapped in XKMS (XML Key Management Specification) formats.

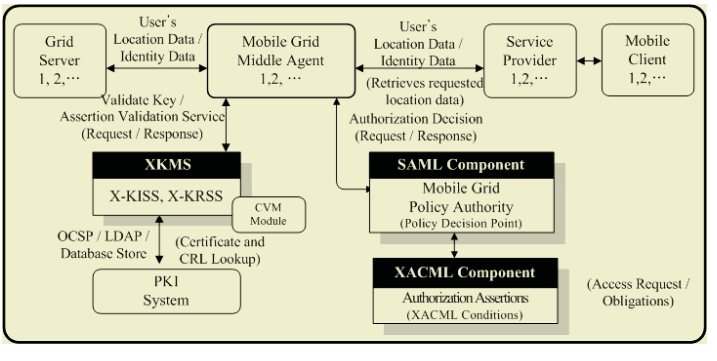

Fig. 3. Security Framework for Open Mobile Grid Middleware

XML encryption allows applications to encrypt part or all of an XML document using references to pre-agreed symmetric keys. The WS-Security, endorsed by IBM and Microsoft, is a complete solution to provide security to web services. It is based on XML signatures, XML encryption, and an authentication and authorization scheme similar to SAML. When a mobile device client requests access to a back-end application, it sends authentication information to the issuing authority. The issuing authority can then send a positive or negative authentication assertion depending upon the credentials presented by the mobile device client. While the user still has a session with the mobile applications, the issuing authority can use the earlier reference to send an authentication assertion stating that the user was, in fact, authenticated by a particular method at a specific time. As mentioned earlier, location-based

authentication can be done at regular time intervals, which means that the issuing authority gives out location-based assertions periodically as long as the user credentials make for a positive authentication [4,5,8].

4 Test Configuration and Results

Components of the grid security are XML security library, service components API, application program. Although message service component is intended to support XML applications, it can also be used in other environments where the same management and deployment benefits are achievable. The figure for representing Testbed architecture of service component is as follows figure 4.

We will concentrate on the most limited category of wireless Java 2, Micro Edition (J2ME) devices that use Mobile Information Device Profile (MIDP). Applications that these devices understand are midlets. Typically maximum size of a midlet varies from 80-100kbs and user can download six to nine applications to his mobile phone. Midlet is a JAR-archive conforming to the midlet content specification [2]. The server is composed server service component of mobile grid platform package. And the message format is based on Specification of W3C (World Wide Web Consortium).

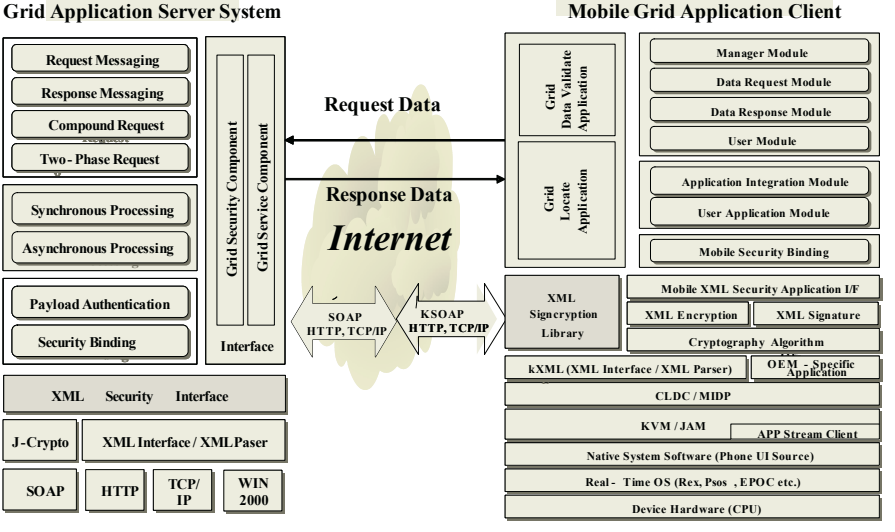

Fig. 4. XML Signcryption Component for Mobile Grid Services

Figure 5 shows the time taken for verification of the signature takes a longer time than the generation of the signcryption value itself. Figure 6 shows in the information in a graphical form. It can be noticed that as the number of iterations increase the amount of time taken per iteration decreases significantly. In the case of Unsigncryption the time taken per iteration is much more than the time taken for signcryption. The process provides both confidentiality and integrity at relatively lesser speed and lesser time as compared to other signature techniques.

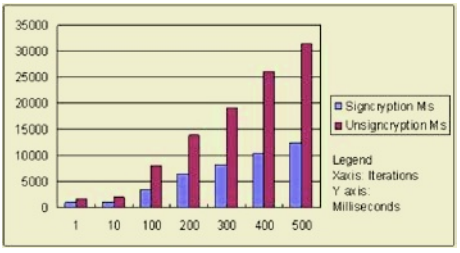

Fig. 5. Time taken plotted against number of iterations for Signcryption & Unsigncryption

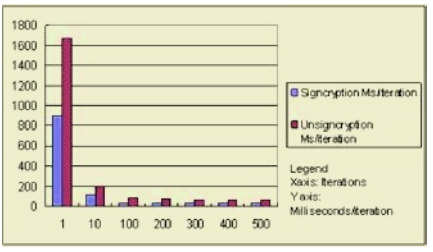

Fig. 6. Average time/iteration mapped against the number iterations

5 Conclusion

Mobile grid services are so attractive that they can cover all walks of life. However, current grid is growing slower than expected. Many problems like accuracy, privacy, security, customer requirement have to be addressed. It should be understood that there is no single universal solution to grid. signcryption technique allows simultaneous processing of encryption-decryption and Signature. It has been proved that the use of signcryption decreases the processing time by 58%. signcryption is being programmed using the field theory. signcryption technique is very efficient as it uses only a single exponentiation for both encryption and signature.

We propose a novel security approach on fast mobile grid services based on current mobile web services platform environment using XML signcryption mechanism. Our approach can be a model for the future security system that offers security of open mobile grid security.

References

1. Miika Tuisku: Wireless Java-enabled MIDP Devices as peers in Grid Infrastructure. Helsinki Institute of Physics, CERN
2. Ye Wen: Mobile Grid Major area examination. University of California (2002)
3. E. Faldella and M.Prandini: A Novel Approach to On-Line Status Authentication of Public Key Certificates, in Proc. the 16th Annual Computer Security Applications Conference (2000)
4. Yuichi Nakamur, et. Al.: Toward the Integration of web services security on enterprise environments. IEEE SAINT '02 (2002)
5. Diana Berbecaru, Antonio Lioy: Towards Simplifying PKI Implementation, Client-Server based Validation of Public Key Certificates. IEEE ISSPIT (2002) 277-281
6. Joonsang Baek, et. Al.: Formal Proofs for the security of signcryption, PKC'02 (2002) 80 – 98
7. Y. Zheng: Digital signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption), Advances in Cryptology – Crypto'97. Lecture Notes in Computer Science, Vol. 1294. Springer-Verlag (1997) 165-179
8. Wooyong Han, et. Al.: A Gateway and Framework for Telematics Systems Independent on Mobile Networks. ETRI Journal, Vol.27, No.1 (2005) 106-109
9. Jang Hyun Baek, et. Al.: An Efficient Two-Step Paging Strategy Using Base Station Paging Agents in Mobile Communication Networks. ETRI Journal, Vol.26, No.5 (2004) 493-496