Securing the transaction by parsing XML file in mobile Commerce

Jyoti Batra Arora
Assistant Professor, Department of Computer Science, IITM Janakpuri, New Delhi, India
jybatra@gmail.com

Abstract

M-Commerce is emerging as ubiquitous technology among the existing wireless medium. It is technique of making transaction using mobile phones. Users are highly dependable on mobile phone because of it's anytime, anywhere features. The transactions using mobile phones are increasing than desktop. Therefore, the performance and adaptability of M-Commerce is highly dependable on security of transaction. Mobile phones use different protocols for their display and programming while making the transaction. WAP, i-mode and J2ME technologies are used for programming for making transaction. The XML file is used to send data during transaction. The XML processor takes more time to encrypt which leads to breakdown the security during transaction. This paper has defined the code to parse XML file which reduces it size so that data during transaction would be sent with ease and fast. To enhance the security, XML file is encrypted before parsing. This paper has the code for encryption and parsing of data during transaction. The code is written in XML and J2ME as these technologies can easily run on multiple platform.

Keywords: WAP,i-mode,J2ME,XML,Parser

1 Introduction

Mobile phones are emerging with greater speed in terms of techniques and design in wireless environment. Mobile phones are more popular than desktop because of its ease of availability, uniqueness, small size and anytime work. Users take advantage of this aesthetic consideration. Mobile phones use Wireless Application Protocol (WAP), i-mode and J2ME as programming protocols to make transaction. The network connection is required to process the data in WAP technology. The request is encrypted in WTLS and decrypted as TLS data which make encrypted data more vulnerable.

Yaun and Lung (2006) showed that J2ME applications offer more features and security than WAP. They stated that one should look no further than J2ME applications for high level mobile security code. A proprietary DoCoMo scheme is used in i-mode to encode radio towers and digital radio packets are sent between handset. The information about this scheme is not available. Java platform make users to develop portable code that can run on multiple platform. It has been designed to strike a balance between portability and usability.

The security risk while making transaction in mobile commerce is categorized in technical and non technical risks. Technical risks identification integrity, message integrity and risk related to data, platform and software. The non-technical risks involve risks related to privacy, regulatory, anonymity, loss of personal information, trust, confidentiality, access. It also includes access to infra structure and concern of government in development of mobile commerce in the nation. The identification integrity refers to the signature element found in message to infer from where the message is originating the message integrity points to detail to establish that no third party opened, modify or alter the content. The technical risks have more concern of sender and service. The risk of theft or misuses of personal information and repudiation of transaction are major issues for both. Data in M-Commerce is secured by using encryption technology which is vulnerable to attack. The technical security risks can also be seen into impact data in a mobile commerce transaction platform to facilitate data communication and necessary protocol and software for this communication. Dorman (2001) poised that vary nature of wireless computing is the generation of adhoc network for communication. Wireless connection can be easily broken-down without adhoc network. This can be done at transport layer of network mobile user move through many different cells and adhoc network and communication is handed off from domain to domain. During this communication a single malicious domain can facilitate malicious download of data or program. As secure DNS is not deployed wireless communication, therefore it is easy to implement stealthy attack to change the dynamic information for benefits of malicious user. Data is exchanged between mobile user and network during the realization of different services. This is the point where information can be altered or stolen. The reason behind is that WTSL does not follow rigorous authentication procedure and do not perform standard check after the establishment of connection. It helps the attacker to redirect transaction request without the knowledge of user. Most websites are not configured to deal with intermittent service failure, which becomes an advantage to attacker. The data security is the major

issue in security of M-Commerce. In March 2000, AT&T wireless and sprint PC's sent user's phone number to the website which they accessed from their web enable wireless phone. These websites could track users and can used for offline direct telemarketing. The weak state of privacy protection is evident in the business setting too.

Stuart and Bawany (2001) defined different software flaws in mobile transaction security. The first flaw is in the logic of a program and its implementation. The second flaw is use of low-level language for the development of application for mobile device. Thirdly, the physical limitations of these devices like limited power bandwidth and processing cycles may impose security and performance trade off. Finally security features available in advanced language like JAVA is ignored by vendors due to developmental time constraints. In M-Commerce cookies are replaced with locator devices and these devices facilitate the tracking and monitoring the individual's activities. The location information can be captured even when device is merely on and not handling any call. Rose (2001) stated three major issues for necessity of trust. They are diverse nature, the intensive use of supply chain, the empowerment of workers and self-directed team work. One has to manage technological and business risks to get a satisfactory level of trust.

Simpson (2003) in his research showed that there are many incidents where personal information is disclosed without proper consent. Trust is the center of security risk in the case of mobile transaction. Green (2004) in his report said that consumers are more worried about their privacy and potential intrusion in M-Commerce environment.

To grow and develop M-Commerce in a country National IT infrastructure, Education and Awareness of citizen has important role to play. In short, future trends clearly indicate that the device manufacturers as well as service and infrastructure providers will keep adopting the WAP standard. The major issues related to use of infrastructure are skills availability of radio frequency, technology and service cost. A minimum standard availability can hinder development. Government is concerned with regulatory framework in development of M-Commerce.

Different mobile devices use three major techniques for making transaction and programming standards-J2ME, WAP and i-mode. J2ME is Java technology customized for embedded devices with limited processor, memory display and input capabilities. Java with XML creates a powerful combination of portable code and portable data. J2ME has built in consistency across products in terms of running anywhere, anytime and over any device. Java technology in mobile devices has two advantages: security and disconnected transaction with wireless synchronization.

WAP allows a relatively easy and unproblematic integration of mobile applications into existing Internet services. Web servers can be modified with the help of suitable software to offer WAP functionality. WAP devices uses SSL between web server and gateways a potential security breach. But if SSL is striped out and data is placed into another security format, the data would be potentially exposed on the carrier's network. Java technology uses Java application which can run on a mobile even when it is disconnected or out of coverage area. The i-mode is basically used by Japan which has advantage over WAP. The official content providers do not have to install own payment mechanism. It works on iHTML which is a subset of HTML so that internet content can be transferred to i-mode with less problem and low cost. An i-mode is only compatible with i-mode devices.

The major issue is with the problem of Denial of Service and Non-repudiation attack which can be easily overcome by using J2ME with XML. It parses the message to be sent to and by merchant so that only authenticated user can access the data.

This research paper has a pragmatic approach to secure adoption model for M-Commerce for generic mobile devices using J2ME with XML, where the parsing size of XML is reduced which makes secure transactions by controlling the delay and error in mobile transactions.

Features of XML required for parsing

With the expansion of wireless world the server vendor serves WML over WAP and HTML over HTTP. XML with its multi-tire structure overcomes the limitation of HTML and protects the information distributed on web. Multi-tier architecture of XML described that a standalone client can communicate with the applications on server in different ways. The client can use RMI to manipulate the remote object and make HTTP connection. The main advantage of using standalone client than browser is the chance to provide a rich user interface whereas the main limitation is the difficulty of client installation and maintenance.

XML can be used on different platforms such as UNIX, Linux, Solaris and Microsoft Windows and can work on mainframe systems. XML with J2ME plays an important role in protecting the data not only stored within devices but also data that transferred over the network. XML with J2ME provides security solution for confidentiality, non-repudiation, authentication and integrity. It has features such as

flexibility, extensibility and compatibility which make its better use for secure transaction in mobile devices. XML due to its structure is redundant and large overhead. It evolves in most important format for data exchange in distributed network.

2 Need of parsing XML file

The security of M-Commerce should be strong enough to protect different transaction from abuses and to the user's trust. XML based services have two challenges i.e. security and performance. XML based security threats are emerging and consists of mainly data compromise, XML based DoS (Denial of Service) and Content based attack.

The computer hardware can understand only one language. When the code is written in XML, hardware has no clue what it means. Parsers as software convert the code into hardware recognizable form. It is the process of analyzing XML document and generates the internal and structured data representation to be accessed by application program. The main aim of parser is to transform XML into a readable form.

XML processing function includes XML parsing with schema validation. It parses the XML message and checks for its validation. The result of XML parsing should provide enough support for XML query, XML security. It transforms the text into a data structure such as semantic checking, code generation.

XML Encryption (2002, 2003) described XML signature and encryption as widely used and building block technologies. It is easy and a natural way to handle security in data interchange application. XML security system consists of XML parsing with schema validation, XML signature and XML encryption. If XML is used at server side then it is consider as a data exchange format. Sending the data from client to server has many advantages such as self-describing data and loosely coupling between the client and server.

3 Literature Review Of Parsing Techniques

Encryption is done through symmetric and asymmetric algorithm. Symmetric cryptographic algorithm does not provide authentication, message originality and non repudiation the same secret key is used for encryption and decryption which makes a loop hole in security but in business transaction one is associated with different business partners so they cannot give the share the key with everyone. Symmetric algorithm encryption can be divided in to two types: Block cipher and Stream cipher. Block cipher encrypts the plain text in fixed packet length of 64 or 128 bits long whereas stream cipher uses key to break down the function and generate a key stream followed by XOR operation between plain text byte and each byte of key stream to generate the cipher text. The length of each key is generally 8 bits long. RSA, SEAL and SOBER algorithms uses stream cipher techniques and DES and AES uses block cipher techniques.

Lo etal. (2008) poised that encryption does not provide full end to end protection. It should provide some additional techniques to make the mobile device safe and secure. The combination of asymmetric and symmetric cryptography can provide robust result. Encryption can reduce the size up to 28%. The best result can be achieved for the combination of encryption and decryption if the size of XML file is large up to 200 kb before encryption. Simulation reduces the size of decryption. Encryption achieves the confidentiality of algorithm and keys. Encryption algorithm based on confidentiality of algorithm is kept secret whereas encryption transform algorithm based on confidentiality of key made public. The algorithm uses the key is kept secret. According development of W3C in September 2002 the aim of XML encryption is a data encryption that uses XML to describe Web resources; it can be HTML, XML, JPEG file or any file that can be any element in XML file. Java crypto extension with SAX gives better results as compared to traditional method to preserve integrity and confidentiality. XML encryption does not define a new algorithm, but a combination of XML technology and existing encryption algorithm.XML encryption generally includes three entities: Application, Encryption, Decryption. The decryption parses the XML file in the package element and decrypts it. The verification of result of decryption and its synthesis is done by application processing which follows a standard and effective method.

Parsers can be in different format and style such as free standing software, libraries, modules and classes. A validating parser compares a set of specific rules for specific XML file and gives decision about default values and validates data types whereas a non-validating parser provides the code for quick check for all basics. During development cycle, validating XML parser ensures the documents generated by server are clean. Apart from above parsers computer hardware uses standalone parser which requires separate package to parse XML. These parsers serve little purpose as most of the editing software has inbuilt parsers.

XML parser is software or Java class which reads XML file and checks for its conformance to standard and validates it. It generates a structured tree to return the results to browser and has similarity to processor that determines the structure and properties of data. XML parser deciphers the XML code and provides

the information to the program for reading the files. Wei Wang (2007) in his paper has defined two key challenges i.e. Security and Performance for deployment of XML based services. The security issues lead to development of XML security processing functions, XML encryption and XML signature to provide element level protection. Increase in XML traffic and increase in consumption of system resources by XML processing overloads the system and decrease the performance of XML based services. The XML devices require advance XML processing algorithm to support high performance services.
Parsing can be done either through algorithm or by programming interface. Papakonstantinou (2003) poised Tree parsing algorithm which parsers the XML message into a tree name where element name and attribute values are represented as nodes. Nag (2004) in his paper defined the tokenized XML format as memory efficient parsing algorithm. The XML message is cut into several pieces and stored in memory.

Zang (2006) in his paper defined non extractive parsing algorithm which is having a two-tuple integer array for each character string in XML message. The first tuple is used for offset of the string and other is used for the length of string. This is very useful in memory usage and XML query, but does not support XML security processing.

These three algorithms are well designed but do not aim at specific XML security processing such as XML encryption and XML signature. The strict syntax and parsing requirements make necessary parsing algorithm extremely simple efficient and consistent. The further research detail is on the XML paring with secure feature.

XML parsing can also be done through either. DOM (Document Object Model) or SAX (Simple API for XML). The new and other developed model use the aforesaid programming interfaces as their base. These models are actually API used by user for processing XML document with Java. XML uses Document Type Definition (DTD) with extension .dtd to provide the specification to text element in a model document. It specifies the attribute and the valid value of element. XML processor includes Tree based APIs and Event based APIs to read the document.

DOM model (2004) in their paper described DOM as a tree based API for accessing XML document. The XML document is represented as tree structure where XML tag is a node. Data is stored as a tree in memory which allows navigating the tree and serializes it back. This is also a drawback as it requires more memory to store the entire document even when only a portion of document is to be processed.

XML tutorial (2005) described SAX as primary event based processing. This reports the parsing event directly to application through call back method. JDOM (Java based Document Object Model), JAXP (Java API for XML processing), Xerces are few types of API supporting both DOM and SAX. These parsers require more memory and are resource intensive.

The other problem during XML parsing is dynamic allocation of memory which is defined by Collado etal. (2008). As the process is not time deterministic, so leads to memory fragmentation and failure to allocate sufficient memory for the operation. They have defined a processor named EXDOM (Embedded XML DOM Parser) using J2ME platform for data analysis on Network Embedded System (NES) and optimal use of memory. It works with environment that has limited memory and computational power and also overcome the problem of predictable real time response. It deals with pooling and reuse of objects, node value retrieval with single tree navigation operation and programming optimization with Inlining method. They have used the basis of Cheng (2006) who said that the set of optimization practices like class merging, elimination of variables or method Inlining reduce the size of codes or heap usage; where reduction in code size decreases the total number of bytes used by program in memory and reduction of heap usage indicates the availability of dynamic memory for other application. Wenjun Liu (2010) in his paper defined the web service's architecture and constructional method as a solution to data transmission between mobile clients and web server and XML data parsing by taking care of few issues like mobile devices, small memory capacity and high cost of wireless network. He has described a model which explains the M-Commerce architecture which is based on web service using J2EE_J2ME technology and SOA method. He has used simple parsing of XML. The only difference is that the client uses a specific method of web service which according to client makes no difference with any other method, but actually clients are communicating with deputy classes. He has used HTTP protocol as request/response protocol as all the realization of MIDP support HTTP, so it becomes suitable for all kind of mobiles.

Rami Alnaqeib et al. (2010) in their paper has shown that the different way to reduce XML parsing is to change XML, which is an idea behind less than 19 proposals for binary representation of XML document, as the binary representation is faster than textual data. In their paper they have given the conformance test on a number of parsers like Elliotte conducted test and concluded that Xerces is most conformant parser to SAX standard. Mohseni in his performance test showed that Microsoft XML (MSXML) had shortest load time. Among the DOM parser no one is proven as best option.

Ajeet Singh etal. (2012) in their paper described two important security technologies – XML signature and XML Encryption with review of XML key management of public keys to protect the payment information distributed over internet. They have provided a security mechanism that is not covered by SSL/TLS. In their mechanism they have also assumed that the data is parsed in XML.

From the above discussion it has been shown that poor performance in parsing XML file causes the serious obstacle to adopt XML based solution in E-Commerce and M-Commerce. Therefore, many researchers are working also till date to improve the parsing phase even by binary representation of XML document. Researchers are also working on schema specific parsing, where parser is generated to only recognize XML document compliant with the source XML schema specification.

J2ME has different standard libraries to process XML files and different parsers are available for different operating system. The Java standard also has STAX parser which is also not a part of android platform. Android provide XML parsing which is not available in standard Java but has similarity with STAX parser. The pull parser is the best option to use on android platform because it is fast and require less memory as compared to DOMAPI.

4 Limitations of Standard Encryption of transactional data

Encryption of XML document is important to provide end to end security to application which requires exchange of structured data. It is a two step process – the first is to seal the document and second is for a secret key used to encrypt the document. In the first step a secret key is generated using pseudorandom number generator. The XML document is encoded and compressed in form of bytes to reduce the size of cipher text and prohibited the hacker from getting any information related to plain text. In the second step the secret key is encrypted using a special recipient public key. XML encryption is easy and natural way to handle security in data interchange application. The applications transform the data in XML format by using an XML parser which increases the possibility to inject data to cause adverse effect in parser.

The attacker generally attacks the application that does not perform sufficient validation to ensure that user controllable data is safer to parser. If continuously bad data is passed to parser it may crash the parser. Therefore, before parsing it is required to validate and sanitize the user controllable data to ensure that the data is safe for parsing. The encryption is required to protect the data and to prevent non authorized attempts from accessing sensitive data stored on mobile device. This paper uses the data symmetric encryption where same key is used for encryption and decryption. The following is proposed algorithm for coding

Step 1: Create a byte array from the initial password and the initial key.

Step 2: Create a new Secretkey from the key byte array, using AES algorithm.

Step 3: Create a new cipher for AES transformation and initialize it in encryption mode, with the specified key using API method.

Step 4: Make the encryption with API method which results into a new byte array with encrypted password.

Step 5: Use the same key to initialize the cipher in decryption mode.

Step 6: Make the decryption of the Encrypted byte array which results into a Decrypted byte array.

The encryption process takes place through the use of algorithm, complex mathematical functions that are applied to the message and make it unreadable without the decryption key. This algorithm is based on UTF-8 which is variable with encoding and dominant character encoding for WWW. It is compatible with XML, DHTML and XML.

5 XML parsing

The mobile devices use internet connection to make transaction. The most efficient way to transfer data between different platform and technologies is to use XML file. XML parser is required to process and extract XML file. A node is required to process XML file. It can be done through following coding:

```
public XMLNode(int nodetype)
{
this.nodetype=nodetype;
this.children=new.vector();
this.attribute=new Hashtable();
}
```

This node is parent text node which is used to get data by using getAttributeNames() function. The data received is put into file by using attribute.put(). The child node can be generated using aforesaid coding which is required to enter the data. The string data type is used to get the data. Once the data is entered, the next step is to parse the XML file. A generic parser class is defined using Kxml parser.

```
public class GenericXMLParser
{
public XMLNode parseXML(KXmlParser parser, Boolean ignore whitespaces) throws Exception
{
Parse.next();
return_parse(parser,ignoreWhitespaces);}
```

This code help to parse any XML file. The code is tested successfully in lab of Telecommunication Company to see the result which shows that code can parse the file. This code uses kXML parser which is a pull parser to avoid fragility caused by SAX parser. The code takes very less time to execute and allow the safe transmission. The hacker has very less to make any changes in transaction. Parsing makes the small packets of file to fasten the processing of the file. This code of parsing has different effect on different operating system. As explained earlier operating systems effect the transmission of data through mobile devices. This code is very helpful in working with android operating system as DOM and SAX parsers both can work easily on android operating system. Eclipse is used as IDE(Integrated Development Environment) and Java Development kit and Apache Ant are used as command line tool to create, build and debug applications and to control attached devices. These devices should be android devices.

J2ME has different standard libraries to process XML files. Different parsers are available for different operating system. The Java standard also has STAX parser which is also not a part of android platform. Android provide XML parsing which is not available in standard Java but has similarity with STAX parser. The pull parser is the best option to use on android platform because it is fast and require less memory as compared to DOMAPI.

6 Conclusion

XML file is use to transfer the data through mobile device because of features. The parsing of XML file reduces the size of file. The parsing can be done through algorithm and programming interface. The proposed algorithm defines the coding which overcomes the problem of encryption of the key which is stored as string in database. It is required to store the encrypted code not the key. The proposed coding of parsing reduces the size of XML file to transact the data fast and increase the security of transaction. The different operating systems used in mobile phones have different impact on parsing the files. They affect the performance of parser. The further research can be made on parsing techniques with respect to operating systems of mobile device. As the new technology is developing the devices are coming with new and advance operating systems, so this study is not limited.

References

[1] Alnaqeib Rami, Alshammari H Fahad, Zaidan AA, Zaidan BB, Hazza M Zubaida, "An Overview:Extensible Markup Language Technology", *Journal of Computing ,Vol 2, Issue 6* (2010).

[2] Cheng S, "Squeezing the last byte and Last Ounce of Performance On your MIDLETS, http://developers.sun.com/learning/javaoneonline/2006/mobility/TS-3418.pdf, visited on 10/2/2018

[3] Collado E. M., Soto M.A.C, Garcia J.A.P., Delamer I.M., Lastra J.L.M, "Embedded XML DOM Parser:An approach for XML Data Processing on Networked Embedded systems with Real-time Requirements", *EURASIP Journal on Embedded systems,* (2008).

[4] "Document Object model Core 2004", http://www.w3.org/TR/DOM-Level-3Core/core.html, visited on 11/2/2018

[5] Ghosh S., "Add XML parsing to your J2ME application",IBM developer works.

[6] Green P., "Eastern Europe's Foray into M-commerce", The New York Times p. 3.8

[7] Hanslo S W., MacGregor K.J, "Using XML messaging for wireless Middleware Communication", University of Capetown.

[8] Hope-Rose. D., "Successful E-Business Deployment: Beyond Software" (No.COM-14-5080): Gartner (2001).

[9] http://www.micsymposium.org/mics_2006/papers/HuKaoYangYeh.pdf, visited on 20/2/2018

[10] Infoway Dotcom," Mobile OS and efforts towards open standards" (2009).

[11] Lo JLC, Bishop J, Eloff JHP , "SMSSec : an end to end protocol for secure SMS", *Computer Security,27,*2008154-167

[12] Lu J, Zhu X, Peng D, Huo H , "Active XML for Service Discovery in Mobile Environment", *JCIT 6(6),*pp 47-53 (2011).

[13] Mohseni P., "Choose Your Java XMLParser", http://www.devx.com/xml/Article/169, visited on 20/2/2018

[14] Nag B, "Acceleration Techniques for XML Processors," In Proc. of XML (2004).

[15] Singh A., Singh K., Shahazad A., Azath M, Kumar S., "Secure payment information using XML technology", *International Journal of Advanced Research in computer Science and Software Engineering,* Vol 2 issue 5 (2012).

[16] Stuart, D. and Bawany, K., "Wireless Service: United Kingdom (operational Management Report No.DPRO-90741): Gartner".

[17] Elliotte R.H., "SAX Conformance Testing", *Proceedings of the XML Conference.*

[18] Zhang W., Robert A., "TDX: a High-PerformanceTable Driven XML Parser", *Proceedings of the 44th ACM Southeast Conference (ACM SE'06),* pp 726-731 (2006).

[19] XML Encryption Syntax and Processing, W3C-Recommendation 2002, Online available: http://www.w3.org/TR/xmlenc-core/, visited on 22/2/2018

[20] XML tutorial, "Introduction to XML and XML with Java," Online available: http://totheriver.com/learn/xml/xmltutorial.html, visited on 23/2/2018

[21] Young D., "Handicapping M-Commerce: Getting ready for wireless e-commerce" *Wireless Review* pp 24-30 (2000).

[22] Zhang J, "Non-Extractive Parsing for XML," http://www.xml.com.

[23] Zhou1 Yamming, Qu Mingbin, " A Run-time Adaptive and Code-size Efficient XML Parser", Proceedings of the 30th Annual *International Computer Software and Applications Conference (COMPSAC'06),* IEEE (2006).