COPYRIGHT © 2011 IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 01, ISSUE 02, MANUSCRIPT CODE: 110121

JXTA & Web Services Using Secret Key Based Encryption

Sabiha Hossain, Upama Kabir, Shaila Rahman *and* Aloke Kumar Saha

Abstract— JXTA is a P2P (Peer-to-Peer) Semantic Web application, which is aimed to accommodate heterogeneous resource metadata repositories in a P2P manner.,the main focus of research in cellular domain has shifted to "Web Service Security" The aim of this thesis will be to develop a distributed service discovery mechanism. JXTA's P2P provides perfect solution for service (Web Service) discovery and Algorithm for Web Service Security. Here I have implemented an algorithm for web service security by using RSA Cryptographic Library and AES Encryption technology. Because most of the attackers may have easy access to Web Services that do not have adequate protection against unauthorized access. So, as the business needs to be protected against unauthorized infiltration, we need to implement some security measures in the Web Services. RSA Laboratories implemented a 330 bit security algorithm on March 18, 1991 named RSA-100. But that was factored within two weeks. Since then RSA has been improving the strength of the algorithm and the latest RSA has 2048 bit key based encryption system. So, in this thesis I have proposed the implementation of an algorithm that is a composition of RSA and AES Encryption that is believed to be strong enough for today's hardware to be factored with.

Index Terms — Peer to Peer Network, JXTA, Web Service, Encryption and Decryption Algorithm.

1 INTRODUCTION

WEB Services are a set of standards and a programming method for sharing data between different software applications. In other words, Web Services is a standardized way to distribute services on the Internet This thesis focuses on peer-to-peer as a method to combine Web Services and mobile ad hoc networks and to use JXTA as peer-to-peer platform. JXTA is a distributed platform that tries to standardize peer-to-peer. The objective is to provide interoperability between entities in the network, be platform independent and offer ubiquity, i.e. any device with a digital heartbeat can participate. JXTA defines a number of concepts that are common for peer-to-peer networks like peer, peer group and pipes.

This Master's Thesis investigates the possibility to combine Web Services and mobile ad hoc networks using JXTA. Web Services provide methods on how to distribute services over the Internet in a standardized way. The Web services framework is divided into three areas 1. The simple object access protocol (SOAP) that enables communications among Web services;

2. The Web Services Description Language (WSDL) that provides a formal, computer-readable description of Web services; and

3. The universal description, discovery and integration (UDDI) directory that is a registry of Web services descriptions. The aim of this thesis will be to develop **AN ALGORITHM FOR** Web Service Security.

2 RELATED TECHNOLOGY

Mobile embedded devices are small, microprocessor-based consumer products, like hand-held battery operated products such as cell phones, two-way pagers, and personal portable organizers.

2.1 Peer-to-Peer Network Architecture

Distributed network technologies try to compensate for some of the limitations of the client/server architecture. They provide a client with an interface to call for services, and so limit the client's knowledge of where to find the services. The earlier distributed network technologies like CORBA and DCOM are highly advanced, and are to extensive and heavy for embedded devices

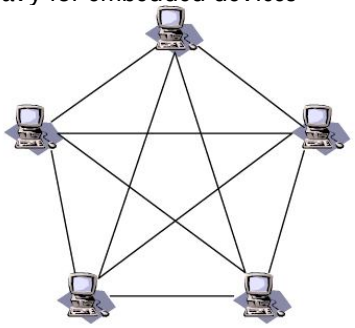

Fig. 1: Basic Peer-to-Peer architecture

- ***Sabiha Hossain*** *is with the Department of Computer Science and Engineering, University of Asia Pacific (www.uap-bd.edu), Dhanmondi, Dhaka-1209, Bangladesh. E-mail: Sabi_up18@yahoo.com.*
- ***Upoma kabir*** *is Associate professor with the Department of Computer Science and Engineering, University of Dhaka, Dhaka-1209, Bangladesh. E-mail: Upoma2@gmail.com.*
- ***Shaila Rahman*** *is Assistant professor with the Department of Computer ence and Engineering, University of Asia Pacific (www.uap-bd.edu), Dhanmondi, Dhaka-1209, Bangladesh. E-mail: srlizauap@yahoo.com*
- ***Aloke Kumar Shaha Head****, Department of Computer Science and Engineering, The University of Asia Pacific,Dhanmondi,Dhaka-1209,Bangladesh*

2.2 Hybrid Peer-to-Peer Architecture

The notion of peer-to-peer has been extended to cover a range of protocols and solution that does not fully satisfy the pure peer-to-peer definition. Many peer-to-peer protocols have introduced a central element in the peer structure to be able to offer a consistent connection.

2.3 Gnutella

Gnutella is a program that offers sharing, searching and downloading of a large amount of file types. Unlike Napster, the Gnutella protocol does not maintain any form of central caches and does not offer a new naming policy to deal with the dynamic client IP addresses.

2.5 Napster

The Napster protocol is composed by clients and servers, and seems in the first place to be nothing like a peer-to-peer networking application. The reason why it Napster is introduced to be the originator of the peer-to-peer paradigm is that it is the first service that take advantage of the possibly enormous amounts of free storage placed in the Internet clients.

3 JXTA

JXTA technology is a set of simple, open peer-to-peer protocols that enable any device on the network to communicate, collaborate, and share resources. JXTA peers create a virtual, ad hoc network on top of existing networks, hiding their underlying complexity. In the JXTA virtual network, any peer can interact with other peers, regardless of location, type of device, or operating environment - even when some peers and resources are located behind firewalls or use different network transport protocols.

3.1 JXTA protocols

At the highest abstraction level, JXTA technology is a set of protocols. Each protocol is defined by one or more messages exchanged among participants of the protocol. Each message has a pre-defined format.In this regard, it is akin to TCP/IP. Whereas TCP/IP links Internet nodes together, JXTA technology connects peer nodes with each other.. So is JXTA. Moreover, JXTA technology is transport independent and can utilize TCP/IP as well as other transport standards.

- Peer Discovery Protocol
- Peer Resolver Protocol
- Peer Information Protocol
- Peer Membership Protocol
- Pipe Binding Protocol
- Endpoint Routing Protocol

3.2 JXTA Architecture

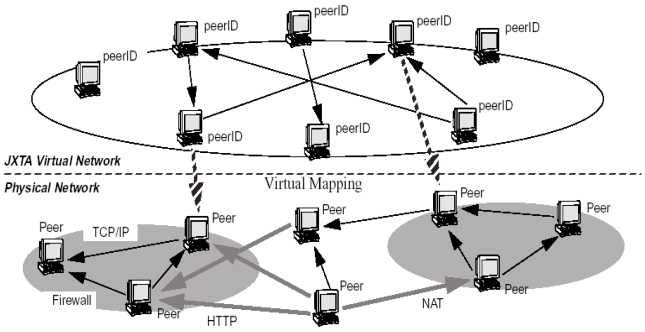

Fig. 2: JXTA Architecture

4 WEB SERVICE

WSDL describes Web services starting with the messages that are exchanged between the requester and provider agents. The messages themselves are described abstractly and then bound to a concrete network protocol and message format. Web Services Description Language (WSDL) is an XML based specification Simple extensions to existing Internet infrastructure can implement Web services for interaction via browsers or directly within an application. The application could be implemented using COM, JMS, CORBA, COBOL, or any number of proprietary integration solutions

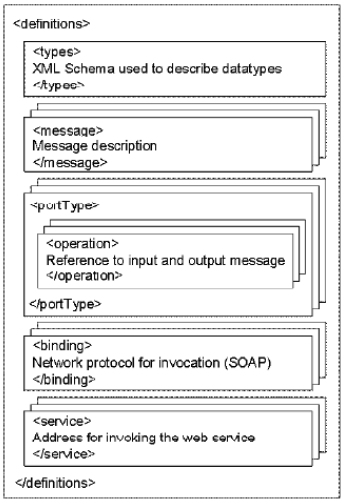

Fig. 3: The structure of WSDL document

Integration of Web Service with JXTA

For Services deployed in JXTA or Web Services Environment to be able to find each other & communicate, we have to do the Gateway Implementation. The Gateway does two major things:

- Communication protocol transformation

- Service Advertising between JXTA & Web Services environment communication protocol transformation

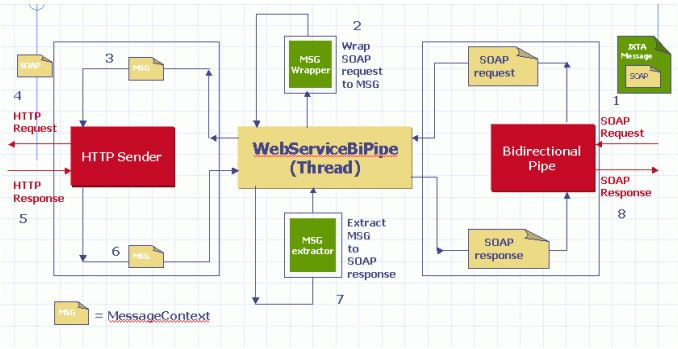

Fig. 4: Advertising between JXTA & Web Services environment

5.1 JXTA to Web Services

When the Gateway receives the advertisement from a *Fig. 4: Service invocation from a JXTA network*

JXTA peer, it translate the JSDL associate with the JXTA peer's service to WSDL, and register the WSDL into UDDI, Services in the Web Services environment can find the "JXTA" service as a "Web" Service on the Gateway, and invoke "JXTA" service by sending SOAP message to the Gateway, the Gateway will transfer the SOAP request in JXTA protocol to the JXTA peer on which the real service is deployed.

5.2 Web Services to JXTA

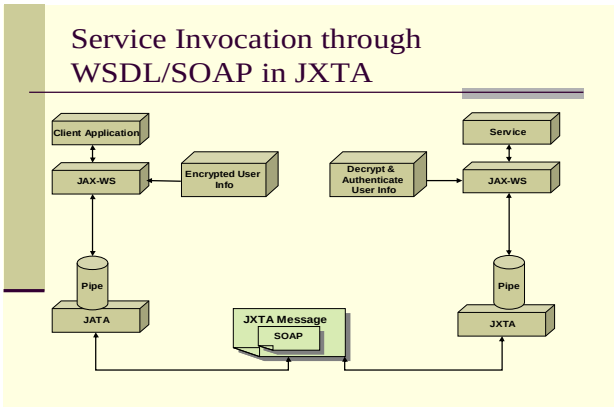

Fig. 5: Service invocation from a JXTA network

When the Gateway receives a Web Services registration request in Web Services environment, it translate the WSDL into JSDL and does the JXTA advertisement about this service in JXTA environment, peers in JXTA environment can find this "Web" service and invoke this "Web" service by sending SOAP request to the Gateway, the Gateway will transfer the SOAP request in HTTP protocol to the Web Application server on which the real web service is deployed.

5.3 Service Invocation from a JXTA Network

The use of Web Services in a JXTA network involves some complications since JXTA does not consider how services, other than core services, are invoked. Any service invocation is possible, including opening direct socket connections to the service, performing Remote Method Invocation (RMI) on a remote service object or simply sending messages to the target peer formatted in accord with the Simple Object Access Protocol (SOAP) document model. The Module Specification Advertisement exposes the information on how to communicate with the service, but no standard for service invocation has been adopted by JXTA.

6. WEB SERVICE SECURITY

The WS-Security specification provides ways to add security headers to SOAP envelopes, attach security tokens and credentials to a message, insert a timestamp, sign the messages, and encrypt the message. The protocol ensures authentication with security tokens. There are three types of security tokens, namely Username/password, Binary, and XML tokens, which can be attached to WS-Security header.

6.1 Web service related security specificaions

1. Terminology
2. Quality of Protection.
3. Namespace
4. ID Refferences
5. Security Header
6. Security Tokens
7. Token References
8. Signature
9. Encryption
10. Decryption
11. Security Timestamps

6.2 RSA Encryption

In 1977, Ron Rivest, Adi Shamir, and Len Adleman developed the public key encryption scheme that is now known as rsa, after their initials. The method uses modular exponentiation, which can be performed efficiently by a computer, even when the module and exponent are hundreds of digits long. The public key is a modulus m and an exponent e. A message is represented by a number c between 0 and m-1. (If the message is longer, chop it up into pieces and encrypt each piece.) Raise c to the e power mod m and transmit the result.

6.3 AES

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor,[the Data Encryption Standard (DES).

6.4 Encryption Decryption procedure

- Client->
  RSA Signing Private Key
  RSA Exchange Public
- Server->
  RSA Signing Public Key
  RSA Exchange Private Key
- Secure Login (Single Sign on or Secure Login).

Client:

1. Get the key that both client and server knows
2. Append a random string of 32 bytes with it.
3. Append timestamp with it. This is User Info.
4. Encrypt this string using RSA Signer (Client's private key).
5. Append the encrypted string with User Info. This is Signed User Info.
6. Create an AES session key (256 bytes). Use AesEncrypter for this.
7. Encrypt the session key using RSA Encrypter (Server's public key).
8. Encrypt the signed user info using AesEncrypter.
9. Append encrypted session key with the encrypted signed user info. This is the Secure ID

Server:

1. Get the encrypted session key from first 256 bytes of UID.
2. Decrypt the session key in bytes using RSA Encrypter (Server's private key).
3. Decode the session key from byte array to string.
4. Set the session key to the SessionKey property of AesEncrypter.
5. Decrypt the remaining part of the UID using AesEncrypter.
6. The readable decrypted signed user info will be visible. Now separate the user id, random, timestamp and signature values from this string.
7. Get the user id, random and timestamp in a string separated by "&".
8. Use RSASigner (Client's public key) to validate the signature. Give the above string and the signature as parameter.

6.5 Key length vs. brute force combinations

.

Key size in bits	Permutations
8	2e+8
56	2e+56
64	2e+64
256	2e+256
2048	2e+2048

6.6 Total time required for brute force attack

Fastest supercomputer "Cray Jaguar" (Invented in 2009 by DoE-Oak Ridge National Laboratory, Tennessee, USA) can process 1.759 PFLOPS per second.

1 Peta = 1,000,000,000,000,000 = 1000e+5 = 10e+15.

Such a system can break the key of length 2048 bits in 2e+2048/10e+15/60/60/24/365 years = 8.8e+8809 years using brute force attack

7 CONCLUSION

In the beginning of the thesis we investigate encryption Decryption Algorithm by using both RSA Signer and AES Encrypter. Two main obstacles to overcome to achieve the goal of this thesis were identified namely how to distribute web services using JXTA and how to deploy an Encryption algorithm for the secured web service. Tphis paper presents an implementation of a web service security technique using RSA and AES Encryption technology. It will secure the web service provided for any business purpose from almost all known security loopholes. Though the attackers may try to crack, but I believe it will be theoretically impossible using today's hardware to break the proposed security.

ACKNOWLEDGMENT

First of all I am very much grateful to the almighty Allah for giving us the opportunity to take such an interesting topic as my Master's thesis. For my thesis I would like to thank first our supervisor, Assistant Professor **Upoma Kabir,** Department of Computer Science and Engineering, The University of Dhaka. Her encouragement, guidance, inspiration and suggestions allow me to do this research work. I would like to give my heartfelt appreciation and gratitude to **Aloke Kumar Saha** Head, Department of Computer Science and Engineering, The University of Asia Pacific and **Shaila Rahman** Assistant Professor Department of Computer Science and Engineering, The University of Asia Pacific, for their kind consideration and assistance during my thesis work.

I also want to thank my **Husband** for his support during my study period. With his patience and support he made it possible for me to finish my studies and complete this master's thesis.

REFERENCES

[1] Traversat and al ,The Project JXTA Virtual Network, May 2001. jxta.org/docs/JXTAprotocols.pdf,

[2] Traversat and al., Project JXTA-C: Enabling a Web of Things, in proceedings of the HICSS-36 Conference, Jan. 2003.

[3] Oaks, B.Traversat, L.Gong, JXTA in a Nutshell, O'Reilly Press, 0-596-00236-X, Sept. 2002.

[4] Web Services Security (WS-Security) Version 1.0 05 April 2002. http://www.ibm.com/developerworks/library/ws-secure/

[5] Comparative Performance Evaluation of Web Services and JXTA for Embedded Environmental Monitoring Systems12th International IEEE EDOC Conference, Middleware for Web Services Workshop, pages: 369-376, September 2008, Munich

[6] World Wide Web Consortium (W3C):"WAP Binary XML Content Format", recommendation, 1999, http://www.w3.org/TR/wbxml/.

[7] Sun Microsystems JXTA-JXME Project: https://jxtajxme.dev.java.net/ (visited on 13.06.2008

[8] WAP Architecture. Wireless Application Protocol, Architecture Speci- _cation, 12 July 2001. http://www.openmobilealliance.org/tech/af_liates/wap/wap-210-waparch- 20010712-a.pdf

[9] WorldWideWeb consortium. http://www.w3c.org

[10] Business Explorer for Web Services, http://www.alphaworks.ibm.com/tech/be4ws [Chandana et al., 2003] C. Subasinghe, D. Cooray, N. Sadeep, L. Kumara, Wonder Room for Easy Web Services Invocation, Department of Computer Science and Engineering University of Moratuwa, December 2003

[11] Web Services in Natural Language: Towards an Integration of Web Service and Semantic Web Standards in the JXTA Peer to Peer Environment P. Contreras, D. Zervas and F. Murtagh, CS, RHUL (2005 May 18)

[12] Elenius, "Resource Discovery with JXTA and OWL-S" and Masters thesis, http://www.ida.liu.se/~daele (site visited 2005 May 18).

[13] Englmeier, "Storybooks in natural language for Web Service Choreography", WSTalk report, 2005 May 18.

[14] Hussain Hajamohideen, A Model for Web Service Discovery and Invocation in JXTA, Thesis, Department of Telematics, Technical University Hamburg-Harburg, March 2003.

[15] InstantP2P Project Home. Website retrieved on September 12 2003. http://instantp2p.jxta.org/servlets/ProjectHome

[16] C. Peltz, Hewlett Packard, "Web Services orchestration: a review of emerging technologies, tools, and standards", January 2003. devresource. hp.com/drc/technical_white_papers/WSOrch/WSOrchestration.pdf (site visited 2005 May 4).

[17] Changtao Qu and W. Nejdl, "Interacting the Edutella/JXTA peer-to-peer network with Web Services", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), IEEE Computer Society, 7 pp., 2004.

[18] Security. (2001). Security and Project JXTA. Retrieved January 25, 2003, from http://www.jxta.org/project/www/docs/SecurityJXTA.PDF

[19] Traversat, M. Abdelaziz, M. Duigou, J. Hugly, E. Pouyoul and B. Yeager (2002). Project JXTA virtual network. Retrieved January 20, 2003, from http://www.jxta.org/project/www/docs/JXTAprotocols_01nov02.pdf

[20] Waterhouse, D.M. Doolin, G. Kan and Y. Faybishenko, "Distributed search in P2P networks", IEEE Internet Computing, Jan.-Feb. 2002, 68-73.

Sabiha Hossain has been serving as a Lecurer in the Department of Computer Studies in Dhaka Residential Model College since February 2008. She graduated in Computer Science and Engineering from The University of Asia Pacific in 2007. Her research interest includes JXTA and RSA Encryption. She also completed her M.Sc. Engg. (CSE) from The University of Asia Pacific.

Upama Kabir obtained her MSc degree from the Department of Computer Science, University of Dhaka, Bangladesh in 1999 and her MS in Computer Science and Engineering from University of New South Wales, Australia in 2005. She worked as a Lecturer (1999–2003),as Assistant Professor (2003–2007), and has been working as Associate Professor from 2007 in the Department of Computer Science and Engineering, University of Dhaka, Bangladesh. Currently she is pursuing her PhD in Concordia University, Canada. She has received several academic awards. Her research interests include parallel processing and distributed systems and computer networking. She has several research publications in national and international proceedings and journals.

Shaila Rahman joined in The University of Asia Pacific (UAP) at 1999 after completing her M.Sc from Dhaka University (DU). She secured 4th position in M.Sc. She also secured the 4th position in B.Sc (Hons) in Applied Physics & Electronics from the same institution. Shaila Rahman teaches courses on Computer Networks, DataCommunications, Information Systems, Microprocessors, Assembly Language, Computer Interfacing, Digital System Design, C/C++, Data Structure and Algorithms. She is conducting the course Mobile Communication in Masters Program of CSE (MCSE). Her current research interest includes Computer Networks and Distributed System, Wireless Networks, Wireless Ad hoc network, Sensor Network, Network Security. She supervised the thesis works of several undergraduate students at UAP. It is praiseworthy to mention that more than fifteen thesis groups in undergraduate level completed successfully under her acute supervision. Her research works published in IEEE, ICCIT, NCCPB, ICCPB. Ms. Rahman has also published two journals on Cryptography and Outsourcing. Ms. Rahman serves as acting head when the head of the department remains on leave. She also serves as an external examiner in the CSE department of Dhaka University. Moreover, She is the convener of the Cultural and Debating club. She is also member of Research and Publication Unit and Programming Contest Club.

Aloke Kumar Saha is Head of Computer Science and Engineering Department of University of Asia Pacific (UAP), Dhaka, Bangladesh. He usually teaches courses on Digital Logic Design, Numerical Methods, Data Structures, Discrete Mathematics, Computer Graphics and Basic Electrical Engineering. His current research interests are Algorithm, Artificial Intelligence and Software Development. For more than 13 (Thirteen) years, he is also working with the undergraduate students of UAP, as a part of their paper works, on the software development and implementation, Bi-Directional Heuristic Search Algorithm etc.