



Secure your Web Services

by Nitin Gupta

Introduction

In this article, we look at the issues involved in securing Web Services and various technologies available for the same. We will also explore the security aspects in relation to the interoperability. We will take a look at the new standards being developed for securing Web Services that will provide standardized security services in future. We will also take a quick look at some commercial products available for providing Web Services security. We will also take a look at how Intel is contributing to Web Services Security domain through various initiatives.

This article assumes that the reader is somewhat familiar with the Web Services architecture, IIS and .NET security.

Security fundamentals

There are various security issues related to information security that need to be addressed by any application security solution. These issues become more relevant in a distributed client server environments like Web Services where there information travels over a wide open networking infrastructure. These issues are as follows:

- Confidentiality: This ensures that any third party listening to the conversation cannot read and interpret the data.
- Integrity: This provides receivers with the ability to detect changes to the original message or data. This prevents against intentional or unintentional data changes during transmission.
- Authentication: This ensures that the client or user accessing the information is the correct person.
- Authorization: This ensures that the client or user has the right to access the information.
- Non-repudiation: This ensures that the client or the user cannot deny the use of the information at a later time.

Web Services Architecture

The architecture of Web Services allows the information to be exchanged in plain text due to use of XML/SOAP over HTTP, which is the most preferred transport protocol. This information can be easily intercepted and interpreted by a third party. So providing security becomes even more important.

The above-mentioned security services can be provided at either the transport level or at the application level using SOAP security. This leads to some differences in the various security mechanisms that can be used because all of a sudden the security becomes tied to the capabilities of Web Services provider platform capabilities and effects interoperability as discussed below.

Security in .NET environment

Web Services in the .NET environment are hosted by IIS and thus the built-in security features of IIS can be leveraged in this environment.

- SSL can be enabled for HTTP to provide confidentiality and integrity of the data being transferred over HTTP. Non-repudiation services can be provided by enabling use of client-side X.509 certificates (Use of client-side certificates is optional in SSL protocol). Once SSL is enabled, all the data sent over these connections will be encrypted and signed.
- IIS provides multiple authentication mechanisms: Basic, Digest, Integrated Windows Authentication (NTLM/Kerberos), or X.509 certificates. Any of these authentication mechanisms can be enabled for the particular directory that hosts the Web Service and this will in turn allow client to present the appropriate credentials and authenticate to the IIS. In addition, the web.config file for the Web Service needs to be modified to indicate that "windows" authentication should be used. Also, anonymous access needs to be disabled in IIS.
- To provide authorization, you can use "Code Access Security" mechanism provided by .NET. This mechanism essentially provides the user identity of the user invoking the Web Service in the Web Service method being invoked. You can explicitly check whether the user has been authorized to access the Web Method after retrieving the user identity provided by the client based on the authentication mechanism configured in IIS.

Security in Java environment

- You can enable SSL for HTTP for the Web Services hosted in the Java environment also. This will again provide confidentiality and integrity of the data being transferred over HTTP.
- But the only authentication mechanism available in this environment is basic authentication. This will require you to add appropriate user names and passwords to the appropriate web server.

Web Services related security standards

Another way of securing the Web Services is by securing the data that is being transferred over the underlying non-secure transport protocols like HTTP. We can do this by various techniques discussed below.

SOAP is a simple XML based text message format that is used to build Web Services requests and responses. The SOAP message is broken up into two portions: the SOAP header and the SOAP body. The header is used to hold any potential metadata associated with the request, while the body is used to hold the basic data contents that go along with the message.

To provide message confidentiality, the SOAP message body can contain encrypted message data and the header can contain the session key encrypted

with the private key of the message sender. At the receiving end, the session key can be extracted by using the public key of the sender and this session key can then be further used to decrypt and extract the data contained in the SOAP message body. This procedure also provides the guarantee that the message came from the particular user because only that user would have access to the private key that encrypted the session key.

More information about XML encryption can be found at [XML Encryption Syntax and Processing](#) and about XML signature can be found at [XML Signature Syntax and Processing](#)

Similarly, to provide the message integrity, a message digest for the SOAP message body can be generated and sent in the SOAP header. At the receiving end, this hash can be regenerated by the receiver for the SOAP message body and compared against the hash value received in the header. If these two values match, it ensures that the message has not been altered during transit.

This XML based encryption; signatures and integrity verification can be done with some support from the Web Services stacks both on the server side and client side. More and more toolkits will support these standards as they become more mature and accepted.

Another upcoming standard SAML is going to play an important role in Web Services Security interoperability. SAML, the Security Assertion Markup Language, is a proposed XML-based framework for exchanging authentication and authorization information among disparate Web access management and security products. Using SAML, security information can be expressed as an XML document and securely transmitted from one application to another. It is being standardized through the Organization for the Advancement of Structured Information Standards (OASIS). SAML enables an application to communicate with security systems provided by disparate vendors. SAML defines a vendor-independent XML data format for representing security information. Consequently, software from vendor A can generate information about a user or an access control decision using SAML; this can be consumed by software from vendor B without any disclosure of proprietary algorithms or data formats. More information can be found at <http://www.oasis-open.org/committees/security/>.

Commercial products for Web Services Security

Some independent vendors have developed products aimed at providing authentication and authorization services for the Web Services. This frees developers from embedding authentication and authorization processing code in each individual Web Service. Products such as Netegrity TransactionMinder from Netegrity (<http://www.netegrity.com>) provide policy-based authentication, authorization, auditing services based on industry standards like XML Signature and SAML we have discussed earlier. These products allow use of existing user directories and easy user and policy management. Please notice that these

products still depend on transport level security for data encryption during transit.

Intel and Web Services Security

Intel has been very actively promoting development of an infrastructure to promote adoption of Web Services. Since Web Services security is one of the most important building blocks that needs to be in place for widespread adoption of Web Services in the enterprise, Intel has been doing the following:

- **Driving standards:** Intel is an active member of OASIS WS-Security Technical Committee. OASIS is a not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards. WS-Security defines a set of SOAP extensions which can be used to implement integrity and confidentiality in Web services applications, laying the groundwork for higher-level facilities like federation, policy and trust.
- **New generation processors:** Some of the new technologies like XML signature that are being used for enabling Web Services Security are much more resource intensive than some of the traditional technologies. This increased resource demand can prove to be a roadblock in adoption of Web Services in the enterprise environment. But the new generation IA64 processors provide much better performance for such technologies. Also, Pentium 4 processor with an advanced 800 MHz system bus and Hyper-Threading Technology provides performance suitable for increased demands for Web Services security solutions.
- **Web Services Optimization Tools:** Intel has developed tools to enable Web Services optimization that becomes more critical due to processor intensive nature of the Web Services security technologies as mentioned above. The VTune Enterprise Analyzer is designed to measure and improve in-depth code-level performance of n-tier Microsoft* DNA* and .NET* applications. In addition, VTune Enterprise Analyzer provides support for legacy applications through web services so that developer can use a single tool to analyze mixed applications. Using the tool, you can view HTTP, DCOM, Microsoft* SQL and SOAP response time statistics. This information can be used to optimize your Web Services application.

More information about the VTune™ Enterprise Analyzer for Web applications .Net Edition can be found at

<http://www.intel.com/software/products/vtune/enterprise/overview.htm>

- **Web Services at Intel :** Incorporating Web Services into an EAI/B2Bi strategy

Intel's Information Technology (IT) group realizes that Web Services are a promising new technology and believes they can add value to Intel. Intel

plans to integrate Web Services into its Enterprise Application Integration(EAI) and into its supply chain, which it collectively refers to as Business to Business Integration (B2Bi). Intel has also made investments in other technologies for EAI and B2Bi.

- o **Enabling third party products:** Intel has invested in independent companies to enable Web Services security solutions. E.g. Vordel, an independent software vendor headquartered in Dublin has developed a product that implements open standards to provide essential security and accountability for Web Services. By delivering security and authentication, Vordel enables companies to make use of Web Services, safely and securely. As an Intel Capital portfolio company, Vordel has optimized its solution to take advantage of Intel's most advanced enterprise processor lines, the Intel® Xeon™ processor and Intel® Itanium™ processor.

VordelSecure 2.0 provides organizations with a high performance, scalable, enterprise security management solution to secure their XML communications. It implements XML security standards such as WS-Security and SAML, using a scalable, agent-based distributed architecture

- o **Consulting:** Intel® Solution Services is a worldwide consulting and services R&D organization, specializing in distributed solutions and data center infrastructure. The Web Services Practice, a part of ISS provides design and implementation support for enabling Web Services security. For more information please refer to

<http://www.intel.com/cd/services/intelsolutionservices/asm-na/eng/index.htm>

Conclusion

There are a lot of different technologies available for Web Services security, a lot of which are somewhat platform dependent. New standards are being developed that will allow more interoperability between different platforms and development toolkits. In spite of these issues, Web Services can be secured in a reliable manner and can expose legacy functionality to the outside world allowing increased productivity and functionality.

Looking forward

In the next article in this series, we will cover some other topics related to Web Services like deployment and performance management.

About the Author

Nitin Gupta is a software engineer over ten years of software systems design experience. Nitin holds a Masters degree in Computer Science from the University of Southern California and a Masters degree in Engineering Management from the Oregon Health and Science University. He is also a CISSP. He can be contacted at nitgupta@alumni.usc.edu.



Copyright © 2006 Intel Corporation. All rights reserved. BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Chips, Core Inside, Dialogic, EtherExpress, ETOX, FlashFile, i386, i486, i960, iCOMP, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, MMX logo,

Optimizer logo, OverDrive, Paragon, PDCharm, Pentium, Pentium II Xeon, Pentium III Xeon, Performance at Your Command, Pentium Inside, skool, Sound Mark, The Computer Inside., The Journey Inside, VTune, Xeon, Xeon Inside and Xircom are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

* Other names and brands may be claimed as the property of others.