WEB SERVICES - SECURITY

http://www.tutorialspoint.com/webservices/web_services_security.htm

Security is critical to web services. However, neither XML-RPC nor SOAP specifications make any explicit security or authentication requirements.

There are three specific security issues with web services:

- Confidentiality
- Authentication
- Network Security

Confidentiality

If a client sends an XML request to a server, can we ensure that the communication remains confidential?

Answer lies here:

- XML-RPC and SOAP run primarily on top of HTTP.
- HTTP has support for Secure Socketes Layer SSL.
- Communication can be encrypted via SSL.
- SSL is a proven technology and widely deployed.

A single web service may consist of a chain of applications. For example, one large service might tie together the services of three other applications. In this case, SSL is not adequate; the messages need to be encrypted at each node along the service path, and each node represents a potential weak link in the chain. Currently, there is no agreed-upon solution to this issue, but one promising solution is the W3C XML Encryption Standard. This standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document. You can check it at http://www.w3.org/Encryption

Authentication

If a client connects to a web service, how do we identify the user? Is the user authorized to use the service?

The following options can be considered but there is no clear consensus on a strong authentication scheme.

- HTTP includes built-in support for Basic and Digest authentication, and services can therefore be protected in much the same manner as HTML documents are currently protected.
- SOAP Digital Signature $SOAP - DSIG$ leverages public key cryptography to digitally sign SOAP messages. It enables the client or server to validate the identity of the other party. Check it at http://www.w3.org/TR/SOAP-dsig.
- The Organization for the Advancement of Structured Information Standards $OASIS$ is working on the Security Assertion Markup Language $SAML$.

Network Security

There is currently no easy answer to this problem, and it has been the subject of much debate. For now, if you are truly intent on filtering out SOAP or XML-RPC messages, one possibility is to filter out all HTTP POST requests that set their content type to text/xml.

Another alternative is to filter the SOAPAction HTTP header attribute. Firewall vendors are also currently developing tools explicitly designed to filter web service traffic.

Loading [MathJax]/jax/output/HTML-CSS/fonts/TeX/fontdata.js