

SOAP Client Authorization (Was: Re: IMAP server security vulnerability)

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2008-03/msg00217.html>

- *From:* "Richard Maher" <maher_rj@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 6 Mar 2008 06:51:31 +0800
-

Hi Arne,

Since login is generally not required and in web

Wow, I bet those "Single Sign-on / SAML / Portal / Identity Provider / wssec: username / RPC Security Interceptor" folks must be feelin' pretty stupid right about now! (Let alone all those companies that simply want to use the Browser and prevailing Web architecture as the delivery mechanism for their in-house client/server applications.)

No login reqd for Bank Account management? Travel Agent Interaction with wholesaler? Customer with Supplier? While I agree that most of the web activity at the moment maybe non account-based retail transactions where, as long as you hand over your (or someone else's) credit card details, no further authentication is reqd, but I don't think that should necessarily exclude those who wish to deploy a stronger Authentication or Identity Management capability.

and in web context the users usually do not have an account on the server then the servers username is often what is available.

Sure, and often that is sufficient, especially when the functions that a given server is to provided are clearly defined and rigidly enforced; not much scope for user embellishment through parameters, selection criteria, or dynamic SQL. But I don't wish to limit my options to some "One true way". I, for one, can see many advantages in being able to assume the persona of the client when the server is performing work on their behalf! Not having to try to replicate the OS security checks, and being able to keep an accurate audit trail, are to name but two.

I'll leave it to someone else to argue the merits of not having everyone login to generic SYSTEM or APPUSER accounts.

SOAP Client Authorization (Was: Re: IMAP server security vulnerability)

If users are logged in, then for static content the access log will have the info, and for dynamic content you can do whatever you want.

Huh? I'm talking about a trigger that says "after update on table Account insert into audit (Culprit) values (Session_User);" what are you referring to? What are they logging in to? Apache "access log"? "Static/Dynamic" SQL?

If it is HTTP.

If is is HTTP. "Doctor it hurts really bad when I do this" :-)

How is the username/password presented to the web-service? (In the wsse:token stuff, or plucked out of the URL, or passed as parameters?)

As arguments to a login call.

That's certainly a popular way of doing it, but I thought that with another option, such as http basic authentication, the server would instruct the browser to prompt the user for credentials? And with WSSE who knows?

[Anyway, I've had this post sitting in "drafts" for some time and another post to c.l.j.p reminded me of it. FYI, I'll post that seperately.]

Cheers Richard Maher

"Arne Vajhøj" <arne@xxxxxxxxxx> wrote in message
[news:476ea845\\$0\\$90272\\$14726298@xxxxxxxxxxxxxxxxxxxxxx](mailto:news:476ea845$0$90272$14726298@xxxxxxxxxxxxxxxxxxxxxx)

Richard Maher wrote:

And for those of you who like VMS Auditing; how do you feel about the Server's username being logged against the audit logs for failed access attempts rather than the Client's username?

Since login is generally not required and in web context the users usually do not have an account on the server then the servers username is often what is available.

Or wouldn't it be nice to have a trigger on an Rdb database table that could log the table access into an auditing table using the Session User Intrinsic rather than the System

SOAP Client Authorization (Was: Re: IMAP server security vulnerability)

User?

If users are logged in, then for static content the access log will have the info, and for dynamic content you can do whatever you want.

If it is web yes.

Not necessarily!

If it is HTTP.

HTTPS for transport encryption and a oldfashioned username/password is common.

How is the username/password presented to the web-service? (In the wsse:token stuff, or plucked out of the URL, or passed as parameters?)

As arguments to a login call.

If you are to the advanced stuff you use WS-S, which is signing and encryption at the message level instead of at the transport level.

Ok, but can you explain a little more about the WS-Authorization/Authentication mechanisms involved?

WS-S basically normalize the XML and sign/encrypt it using private-public keys.

Caller can be authenticated that way. Authorization has to be build into the service.

> I guess I was asking

Jan-Erik which method his SOAP implementation was using to pass Client-Authorization so that we could at least have a real world SOAP example.

SOAP Client Authorization (Was: Re: IMAP server security vulnerability)

I don't think I know a public web service that uses WS-S. The situations where it is used are usually "very non-public".

The gSOAP site says that gSOAP supports WS-Security and unless

Jan-Erik's

client doesn't request much except read-only Google-maps or "Give me the weather forecast" stuff, I'm guessing that the target of his SOAP-call

would

want to validate that a) the client is who he says he is, and b) that

he's

authorized to perform the requested action on the requested data. I, for one, am very interested in the codepath for how this is being achieved!

WS-S provides #a but not #b.

Do you have to pass authorization for each SOAP call, or are you aiming

for

a Single-Sign-on mechanism like SAML? The term "Security Interceptors" sounds interesting also.

You can use WS-S with SAML and other. But basic WS-S is just signing the message with the callers private key and the server checking with the public key. I have never worked with SAML, so I can not comment on the authorization part. There are several other WS-something specs that may be relevant.

Who is your "Identity Provider"? How much does it cost? How long do the identities live? How do you prevent Identity-Hijacking a la mode de JavaScript Session-Hijacking? How could one integrate the

Identity-providers

"Identity" with our VMS Usernames?

A lot of the SOAP stuff is system-system oriented and do not use

SOAP Client Authorization (Was: Re: IMAP server security vulnerability)

sophisticated identity stuff.

And I have never heard about a "SYSUAF based" identity system.

How many of you are working on, or have even seen (website please), an application that combines update functionality (not news/sports/weather-aggregators or language translators) from two or

more

disparate, heterogenous SOAP servers and RPCs? WS-AT? "Business

Activity"

transactions? BEA got a debit/credit thing happening with OracleiAS somewhere?

I have seen a lot of SOAP stuff.

None that are public available. As I said earlier, then the interesting stuff is usually not public.

I have not had to work with transaction WS standards – yet.

SOAP by OASIS – talk about a horse designed by committee :-(

SOAP is a W3C standard not an OASIS standard.

(but OASIS do a lot of the other WS standards mentioned)

Arne