What is the point of a Policy Server? (Silverlight)

Asked 15 years, 9 months ago Modified 15 years, 9 months ago

Viewed 864 times

0

I've been messing around with Silverlight sockets and after scratching my head a bit as to why my connections were being denied I realized I needed to set up a policy server. Silverlight connects to the policy server port on the host specified by the socket connection. The policy server returns an XML file designating what access is allowed onto that host.

Am I understanding this correctly? What is the point of this? Couldn't any malicious user simply ignore the policy file and do whatever they wanted?

alt text http://www.netortech.com/Content/policy.jpg

.net silverlight policy-server

Share

Improve this question

Follow

edited Mar 22, 2009 at 23:17

asked Mar 22, 2009 at 22:28

Spencer Ruport

35.1k ● 12 ● 87 ● 150

2 Answers

Sorted by: Highest score (default)

3

Quote:

> Using for cross-domain communication requires guarding against several types of security vulnerability that can be used to exploit Web applications. Cross-site forgery is a class of exploits that becomes a threat when allowing cross-domain calls. This exploit involves a malicious Silverlight control transmitting unauthorized commands to a third-party service, without the user's knowledge. To prevent cross-site request forgery, Silverlight only allows site-of-origin communication by default for all requests other than images and media. For example, a Silverlight control hosted at http://contoso.com/mycontrol.aspx can only access services on that same domain by default – for example

> > http://contoso.com/service.svc, but not a service at http://fabrikam.com/service.svc. This prevents a malicious Silverlight control hosted on the http://contoso.com domain from calling unauthorized operations on a service hosted on the http://fabrikam.com domain.
> >
> > To enable a Silverlight control to access a service in another domain, the service must explicitly opt-in to allow cross-domain access. By opting-in, a service states that the operations it exposes can safely be invoked by a Silverlight control, without potentially damaging consequences to the data the service stores.

EDIT: based on comment/question ...

I'll just give my probably imperfect understanding of the situation, but this makes sense to me.

A browser in general is constrained in what it can route you to, by making it difficult to access any host other than the one serving up http pages. This is true no matter what resource is under discussion. And these constraints need to be applied by inference to anything else that runs in the context of the browser/web page, including Silverlight. So this is just extrapolating an existing mechanism for allowing foreign references.

I'm not sure how you intend to distinguish a "service" from a "socket". Generally services use sockets; there's some process (service or otherwise) sitting on a host watching to make connections on a port; one type of connection is a socket.

Share Improve this answer Follow

edited Mar 23, 2009 at 0:20

answered Mar 22, 2009 at 22:47

dkretz

37.6k ● 13 ● 83 ● 140

1) I'm asking about sockets, not services. 2) This doesn't answer my question. – Spencer Ruport Mar 22, 2009 at 23:09

I just don't see how Silverlight basically asking a host "what can i access" is anything more than just annoying. Malicious apps will just ignore the policy and go for whatever resource they like so it's not preventing anything. I just don't see the point. – Spencer Ruport Mar 23, 2009 at 4:00

I assume Silverlight gets its access to the internet through the browser - it doesn't have (logically) independent access. It looks like you've found out this is true by experimentation. Of course someone can ping any socket at any ip address with other means, but that's always the case. – dkretz Mar 23, 2009 at 5:09

This is just to make sure it can't be done through a third-party web-based application. – dkretz Mar 23, 2009 at 5:10

That seems kind of silly to me. Any malicious user who knows a thing or two about hacking wouldn't bother using a

Silverlight app for that kind of thing even if it were possible. It's nothing more than a nuisance for the rest of us.
– Spencer Ruport Mar 23, 2009 at 10:37

1

I finally figured out one good reason to do this.

Silverlight apps have the possibility of being distributed/executed very quickly. Say, as advertisements on a popular site for example. In that case it would be very easy for someone to use a Silverlight app to run a DoS attack on a host simply by giving it to an advertising provider. However since all Silverlight apps check the policy file for the host first it limits what hosts and services this kind of attack can target.

Share Improve this answer

Follow

answered Mar 23, 2009 at 16:17

Spencer Ruport

35.1k ● 12 ● 87 ● 150