

Re: Is the way i do, secure enough to avoid session hijacking

Re: Is the way i do, secure enough to avoid session hijacking

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2005-05/msg05122.html>

- *From:* "Kevin Spencer" <kevin@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 26 May 2005 15:31:41 -0400
-

Within the AOL LAN, IP addresses are assigned on a per-client-session basis, if I'm not mistaken (at least with dial-up connections). But again, this is not my area of expertise. Still, I understand quite a bit about networks, and I can't imagine why an IP address of a machine inside a network would change within the same client session. It is, again, the "return address" of the computer on the network.

--
HTH,

Kevin Spencer
Microsoft MVP
..Net Developer
Sometimes you eat the elephant.
Sometimes the elephant eats you.

"gerry" <germ@xxxxxxxxxxx> wrote in message
news:OcbpXiYFHA.3152@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

- > are you sure about that ?
- > from what I have read about AOL proxies and what i see in my IIS logs – it
- > seems that this is not true and that there can be multiple ip's for a
- > single
- > client within a session.
- > i don't have the asp.net session id in the log files so i can't be 100%
- > certain.
- > Gerry
- >
- >
- >
- > "Kevin Spencer" <kevin@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
- > news:OLVN9UhYFHA.3184@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- >> Hi Hope,
- >>
- >> Your method looks pretty sound to me. The client's IP address cannot
- > change
- >> between requests. It is, after all, the "return address" for the client's
- >> HTTP messages.

Re: Is the way i do, secure enough to avoid session hijacking

Re: Is the way i do, secure enough to avoid session hijacking

>>
>> --
>> HTH,
>>
>> Kevin Spencer
>> Microsoft MVP
>> .Net Developer
>> Sometimes you eat the elephant.
>> Sometimes the elephant eats you.
>>
>> "Hope Paka" <utezduyar@xxxxxxxxxxxx> wrote in message
>> news:esEDt7gYFHA.2684@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> >I am storing user login information (not password) in the session. I
>> >also
>> >use, cookieless session. I realized that, if someone copy-pastes the URL
>> >after he/she logged in to the system to another person, the other
>> >person's
>> >browser opens as if the sender logged in.
>> >
>> > 1) Person A Logins to the system. (login information is stored in
>> > SQL
>> > Session state)
>> >
>> > 2) Person A copy-paster the url and sends it to person B (format
>> > of
>> > the url is [http://domain/\(sessionid\)/XYZ.aspx](http://domain/(sessionid)/XYZ.aspx))
>> >
>> > 3) When person B opens the URL, its window opens as if person A
>> > was
>> > logged in to the system.
>> >
>> > This is a security threat. I have overcome this by doing the following.
>> >
>> > When user logins to the system, a login ticket is generated
>> > and
>> > it is stored in the session. This login ticket contains two things, one
>> > is
>> > client ip address, the other one is user-agent.
>> >
>> > Then at the each request, I validate if the registered login ticket
>> > information is same.
>> >
>> > If person A sends URL to person B, then I assumed that, person Bs ip
>> > address should be different than person A.
>> >
>> > I found an article on MSND,
>> > <http://msdn.microsoft.com/msdnmag/issues/04/08/WickedCode/> (Foiling
>> > Session Hijacking Attempts). The way Jeff have done is similar to the
>> > one
>> > that i have done. Is this reliable. The only think i wonder is if the
>> > users IP address changes at each request!

Re: Is the way i do, secure enough to avoid session hijacking

Re: Is the way i do, secure enough to avoid session hijacking

>> >
>> >
>>
>>
>
>

• **Follow-Ups:**

- ◆ **Re: Is the way i do, secure enough to avoid session hijacking**
◇ From: gerry

• **References:**

- ◆ **Is the way i do, secure enough to avoid session hijacking**
◇ From: Hope Paka
- ◆ **Re: Is the way i do, secure enough to avoid session hijacking**
◇ From: Kevin Spencer
- ◆ **Re: Is the way i do, secure enough to avoid session hijacking**
◇ From: gerry

- Prev by Date: **Asynchronous Call Back**
- Next by Date: **Re: accessing controls in web forms user control**
- Previous by thread: **Re: Is the way i do, secure enough to avoid session hijacking**
- Next by thread: **Re: Is the way i do, secure enough to avoid session hijacking**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**