

## Re: Chicken and egg issue with Cookie based login?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2005-04/0120.html>

---

**From:** Barry Margolin (*barmar\_at\_alum.mit.edu*)

**Date:** 04/06/05

Date: Wed, 06 Apr 2005 16:16:08 -0400

In article <8rV4e.33657\$f%4.30258@bignews1.bellsouth.net>, "Julio" <julio@lalaland.com> wrote:

> "Barry Margolin" <barmar@alum.mit.edu> wrote in message  
> news:barmar-47DA57.08524906042005@comcast.dca.giganews.com...  
>> In article <deN4e.29753\$f%4.23725@bignews1.bellsouth.net>,  
>> "Julio" <julio@lalaland.com> wrote:  
>>  
>>> MAC = MD5("secret key " +  
>>> MD5("session ID" + "issue date" +  
>>> "expiration time" + "IP address" +  
>>> "secret key")  
>>> )  
>>>  
>>  
>> Cookies are created by the server, not by the client.  
>  
> Barry,  
>  
> Thanks for your input.  
>  
> Of course, a client can create a cookie as well.

I suppose they can, but that's not what the document is talking about.

>  
>> The server generates the hashed cookie and sends it to  
>> the client.  
>  
> So in reference to the W3C document, this MAC is created by the server? Not  
> the client? Then what is the point? In lieu of SSL, how is the user's  
> credentials obtained by the client, hashed and sent to the server? Via a  
> COOKIE!

The credentials are created when the user logs into the server. For instance, when you use web banking, you enter your account number into a

comp.security.misc: Re: Chicken and egg issue with Cookie based login?

login form.

- >
- > *I've seen references to methods where there might be a combination, a*
- > *server created QUID cookie just to initialize it. The client uses this with*
- > *a new client created hashed cookie to pass the credentials to the server.*
- >
- > *Or are you suggesting the above is AFTER the user has been authorized, this*
- > *this MAC is a hashed cookie for the authorized session?*

Right.

- >
- > > *What if you want to allow the same user to login concurrently from*
- > > *different clients (e.g. a husband and wife both checking their bank*
- > > *account balances)?*
- >
- > *This is already handled. Multiple Logins with the same user credential from*
- > *different machines is already managed with administrator IP control*
- > *preferences. This is already designd for BASIC/DIGEST.*
- >
- > *Just trying to incorporate a cookie-based login method now. I've looking at*
- > *how to pass user credentials to a server as safe as possible using*
- > *non-browser popup dialog box BASIC/DIGEST methods*
- >
- > > > *Is the "Secret Key" the user's password and the Session ID the user's*
- > > > *name?*
- > >
- > > *The secret key should be a random value generated at login time; if it*
- > > *were the user's password, it wouldn't be known only to the server, it*
- > > *would also be known by the client.*
- >
- > *So the MAC equation as outlined by the W3C is an authorization MAC for a*
- > *already logged in session?*
- >
- > *That's ok, but that isn't helping. Need to login first. :-)*
- >
- > *Unless I read it wrong, sounds to me, the initial passing of user*
- > *credentials is less important as maintaining a secured authorized session*
- > *key. Is this because it is a one packet transaction client/server exchange*
- > *with a minimum window of hacker hijacking?*

You use SSL to protect individual requests. The MAC is intended to protect a long-lived session that involves multiple exchanges.

--

Barry Margolin, barmar@alum.mit.edu  
Arlington, MA

\*\*\* PLEASE post questions in newsgroups, not directly to me \*\*\*