

Re: Ace Password Sniffer : How does it work ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-08/0959.html>

From: Multicoder4002 (wickedwicked_at_hotmail.com)

Date: 08/16/04

Date: 16 Aug 2004 00:09:46 -0700

"*Vanguard*" <do-not-email@reply-to-group> wrote in message news:<uLIZScZfEHA.636@TK2MSFTNGP12.phx.gbl>...

> "Miha Pihler" <mihap-news@atlantis.si>
> wrote in news:enDB%237RfEHA.3200@TK2MSFTNGP09.phx.gbl:
> > Hi,
> >
> > *This is not true for SSL. If you use SSL all the content (specially
> > using web interface) is transferred in secure way... I don't think I
> > would be using my on-line banking services if what you are saying was
> > true.*
> >
> > *Another protocol that offers same is IPSec. It enables secure
> > authentication and secure transfer of data between server and client
> > (or client and client). Good thing about IPSec is that you don't have
> > to have IPSec enabled application because it happens on Network level
> > not on application level. With SSL you have to have applications that
> > know how to use SSL (e.g. IE browser, Outlook, OE, . etc), but it
> > would be pretty hard to use SSL to secure data exchanged between
> > server and client when you are using e.g. notepad to work on a
> > document. IPSec can do this even with Notepad.*
>
> *With banking, anonymizer.com, or other SSL-secured web sites, they
> maintain the SSL session so your traffic remains encrypted. That
> doesn't have to be that way, however. In Yahoo Mail's case, the login
> page is SSL secured. Once you are done with the secured login, you no
> longer have an SSL session anymore. Look for the padlock icon in the
> status bar. It is there on the login page (if you pick the https:// URL
> for the login page) but it is NOT there once you are on the webmail
> pages. If you used the SSL login page, you get redirected to a non-SSL
> page after the login has been submitted.*
>
> *Note that SSL could still be used even when the current page is not
> SSL-secured, by submitting form data to a SSL-secured page. I believe
> that is how Hotmail's login page works. When you login to Hotmail, you
> are on a Passport.net page and there is no padlock icon in the status
> bar (because you don't yet have an SSL session). When you click the
> Sign In button, the action=["https://login.passport.com/ppsecure/post.srf"](https://login.passport.com/ppsecure/post.srf)*

microsoft.public.security: Re: Ace Password Sniffer : How does it work ?

- > *clause for the <form> tag directs the data for the form with your login*
- > *credentials gets sent to the HTTPS page. So you aren't SSL secure for*
- > *the login page but the credentials are submitted to an SSL-secured page*
- > *(i.e., from the non-SSL page rendered locally in your browser, you enter*
- > *the data and click Submit, your browser connects to the HTTPS site for*
- > *an SSL session, and then the credentials are sent encrypted to that*
- > *other page). I did not see any HTML for Yahoo Mail's Compose web page*
- > *that would submit form data to an SSL-secured page or site, so the*
- > *absence of the padlock icon in the browser's status bar means you are*
- > *NOT on a secure page when composing and sending your message. Your*
- > *login can be secured but your message contents are not.*
- >
- > *Personally I prefer seeing the padlock icon to know if SSL is still*
- > *inuse. That gives a visual clue as to your security. Submitting form*
- > *data from a non-secure page (rendered locally) which then has it sent to*
- > *an SSL secured page or site means you don't know if the transmit is*
- > *secure unless you look at the HTML code. I suppose that submitting form*
- > *data to an SSL page is cheaper than allocating SSL resources up front*
- > *and pending them until you complete the login, but that leaves you in*
- > *the dark as to how secure are your login credentials. My bank always*
- > *establishes an SSL session and it persists so that I continually see the*
- > *padlock icon during my session. They do that deliberately to let you*
- > *know you have a secure connection. Yahoo doesn't need to do that, even*
- > *when using their webmail interface, since they are only securing your*
- > *login, not your message content. Same for Hotmail. If you don't see*
- > *the padlock icon showing you have a current SSL session, you'll have to*
- > *check the HTML code to verify form data gets submitted to an https://*
- > *page.*
- >
- > *I knew that MD5 uses the SMTP commands in the session between the e-mail*
- > *client and the SMTP server (i.e., Javascript is not used). I wasn't*
- > *sure how Yahoo Mail did it for the freebie accounts that do not provide*
- > *POP3/SMTP servers. From Pidgorny's posts and some Googling, yep, it*
- > *seems Javascript get sents from the server to handle the MD5 processing,*
- > *but hopefully a different randomized key is sent by the server on each*
- > *login. You can see the MD5 parameters in the URL that Yahoo sends to*
- > *you when using MD5 (if you log the HTTP session). That's why I'm not*
- > *sure YahooPOPs bothers to run the Javascript that gets sent by the*
- > *server for the MD5 secured login. I thought the key sent by the server*
- > *was a parameter in the URL returned to the client (YahooPOPs). I*
- > *thought that MD5 also only encrypted the password and not the username*
- > *whereas SSL encrypts both; however, the username is included in outbound*
- > *e-mails, anyway, and since that is plain text than any sniffer could get*
- > *the username.*
- >
- > *Outside an organization that is geographically distributed, especially*
- > *across a WAN, where IPsec makes sense, I haven't heard nor experienced*
- > *any public sites across the Internet that provide IPsec support. Most*
- > *end users have trouble figuring out how to configure the e-mail client*
- > *for non-SSL (i.e., standard) connections, some may use an SSL connect,*
- > *if available, and few even bother with x.509 or PGP certificates for*

microsoft.public.security: Re: Ace Password Sniffer : How does it work ?

> digital signing or encryption, so I doubt IPsec is something that gets
> embraced for services to the typical nondescript user community. IPsec
> seems mostly used for same-LAN host-to-host connection (client/server
> and peer-to-peer), WAN connects between routers and gateways, for
> dial-up clients, and Internet access from private networks. I haven't
> seen IPsec used for any e-mail or webmail services. Wouldn't IPsec
> actually require access to the hardware or hosts on which IPsec was
> enabled (so you can load the driver and manage the policies)? Well,
> banks and other secured sites are often hosted by contracted web host
> providers so the client never has access to the hosts to modify their
> networking configuration and policies. A bank doesn't want to redesign
> their web page or manage the web hosting provider's networking should
> they switch to a different web hosting provider. Using security at the
> application level, like SSL, means control over security is retained by
> the client who ultimately provides the services of that site. The web
> hosting provider obviously isn't going to let their customers monkey
> around with their network configuration and policies and let customers
> mangle their IPsec setup.

thank you for these explanations :)