

Re: Security flaw in how Outlook verifies digital signatures

Source: <http://www.tech-archive.net/Archive/Outlook/microsoft.public.outlook/2005-02/3165.html>

From: Roberto Franceschetti (*roberto_remove_n.o.s.p.a.m_tag_at_logsat.com*)

Date: 02/18/05

Date: Fri, 18 Feb 2005 04:55:06 GMT

I forgot to add the link and contents of Outlook's help file...

Please look in particular at the words "This proves to the recipient that the message is from you and not from an imposter"

That is exactly what Outlook is **not** doing... and we're not talking about RFCs and S/MIME there, because as you correctly state, they are used only as guidelines on how to ensure the body is not changed. We're talking about simple verification that the sender is actually who he says he is. That is **not** defined by the RFC you mention. It's just common sense, and whoever wrote Outlook's documentation thought so as well since they have the right idea there. Too bad they did not convey the thought to the programmers...

>From the Outlook help file on 10/21/2004 (the contents may have changed now...):

(<http://office.microsoft.com/assistance/hfws.aspx?AssetID=HP052423541033&CTT=1&Origin=EC010230001033&QueryID=XUI66rUx90>):

Digitally sign messages

Digitally signing a message applies your certificate (certificate: A digital means of proving your identity. When you send a digitally signed message you are sending your certificate and public key. Certificates are issued by a certification authority, and like a driver's license, can expire or be revoked.) (with the public key (public key: The key a sender gives to a recipient so that the recipient can verify the sender's signature and confirm that the message was not altered. Recipients also use the public key to encrypt (lock) e-mail messages to the sender.)) to the message. This proves to the recipient that the message is from you and not from an imposter and that the message has not been altered. Encrypting (encrypt: The process of converting plain, readable text into cipher (scrambled) text. The sender uses the recipient's public key to encrypt (lock) the e-mail message and attachments.) a message is a separate process.

Roberto Franceschetti

"Roberto Franceschetti" <roberto_remove_n.o.s.p.a.m_tag@logsat.com> wrote in message news:_7eRd.99310\$JF2.25917@tornado.tampabay.rr.com...

> *Jeff,*

>

> *Please read the thorough discussion I've been having with your engineers.*

> *We're not talking about the RFC which merely defines what S/MIME is and*

> *how it operates. As you can read from my report with Microsoft, we all*

> *agree that the S/MIME standard is used to ensure the *body* is not*

> *altered. What we're talking about is how Outlook fails to use digital*

> *signatures in verifying that the sender is who he is.*

>

> *If you read thru those emails you'll see how Outlook's documentation*

> *clearly states that digital signatures are also used to verify the sender.*

> *Let's take another example. Let's look at Outlook Express' documentation:*

>

> *******

> *Sending secure messages*

>

> *As more people send confidential information by e-mail, it is increasingly*

> *important to be sure that documents sent in e-mail are not forged, and to*

> *be certain that messages you send cannot be intercepted and read by anyone*

> *other than your intended recipient.*

>

> *By using digital IDs with Outlook Express, you can prove your identity in*

> *electronic transactions in a way that is similar to showing your driver's*

> *license when you cash a check.*

>

> *******

>

> *What do we have here...? Outlook Express will verify that the sender is*

> *actually the same person as the one in the certificate! ...I thought you*

> *said S/MIME and the RFCs did not account for that... This is exactly what*

> *should be happening. Similar documentation is there in MS Office's help.*

> *All email clients I know of perform this basic, simple check.*

>

> *Microsoft Outlook does not...*

>

> *Again, we're not talking about S/MIME and RFCs here, so please don't try*

> *to pawn this off saying "this is done by design", because if it is it's*

> *very poor design... And you ought to make it very clear in the*

> *documentation that digital signatures will *not* behave like ink*

> *signatures identifying the sender, but that they have a misleading name as*

> *the email is not digitally signed, rather only the *body* of the email is,*

> *and that there should be a disclaimer that Outlook will not, unlike all*

> *other email programs, verify digital signatures against the sender's email*

> *address.*

>

> *I do however have to stand corrected on a statement I made in my previous*

> *post about the subject line. There is currently no way that email clients*

microsoft.public.outlook: Re: Security flaw in how Outlook verifies digital signatures

> *can verify that the subject has been modified, Outlook is not the only one*
> *that suffers from this. However this was not in my original report to*
> *Microsoft, and I will retract on that issue as I've been making an*
> *incorrect assumption. I will blame anger and disappointment on my mistake.*
>
> *Roberto Franceschetti*
> *LogSat Software*
>
>
>
> *"Jeff Stephenson [MSFT]" <stephenson@online.microsoft.com> wrote in*
> *message news:twk104pqa12b\$.dlg@jeff.stephenson.microsoft.com...*