

Re: Security flaw in how Outlook verifies digital signatures

Source: <http://www.tech-archive.net/Archive/Outlook/microsoft.public.outlook/2005-02/3138.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 00:57:50 GMT

Let me clarify first that we're not talking about encrypting, but just signing, two very different things. This said, of course the headers cannot be considered as they will change. However digitally signing a document is supposed to ensure that the document is not altered in any way. When applying this to an email, this would mean that not only the body of the email, but also the "From", the "To" and the "Subject" headers should be tested to see if they are modified. Those will definitely not be changed by servers when mail is being routed.

If you feel so strongly about the "From", how would you feel if the subject of a digitally signed email would be hacked instead... What if the digitally signed email now also had a forged subject line... Instead of saying "Accepted" now says "Declined"? I've just "hacked" my original signed message so that it shows "xxxx" instead of "test" in the subject line. The URL is <http://www.logsat.com/Signatures/Hacked3.msg>... Outlook did not even twitch about the hack, it still thinks the email is unmodified.

What good does having digitally signed emails, which are to ensure the integrity of such emails, if a hacker can *FREELY* modify the sender, the recipient, and even the subject, without Outlook providing any warning?

...And let's not forget that Outlook is the *only* package that fails to verify these very important headers. Other email clients, including Outlook Express, work just fine.

To make matters worse, while with a "From" hack an computer-savvy person can go deep down in the certificate to find the real identity of the sender, there's "almost" nothing that can be done to check if the "Subject" line has been modified, as I've just proved can be done in the sample above.

Roberto Franceschetti
LogSat Software

"Vanguard" <use_ReplyTo@domain.invalid> wrote in message news:D9-dnaFF_-08rYjfRVn-tQ@comcast.com...
> "Roberto Franceschetti" <*roberto_remove_n.o.s.p.a.m_tag@logsat.com*> wrote

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

- > in message news:iI7Rd.89419\$qB6.15925@tornado.tampabay.rr.com...
- >
- > *Certificates are not used to digitally sign or encrypt the headers with*
- > *the body of the message. Why not? Because the headers will change with*
- > *each hop the mail takes to its destination. The body of the message gets*
- > *signed or encrypted, and it is the identity of the certificate that is*
- > *used to determine who signed or encrypted the *message* (NOT the headers).*
- > *Digitally signing a message or encrypting it does not prevent spoofing the*
- > *headers. You use the certificate details to determine to whom the*
- > *certificate was assigned that used it to sign or encrypt the BODY of the*
- > *message, not the headers.*
- >
- > *If you had changed any portion of the BODY of the message then the*
- > *certificate would've been invalidated and you would have seen a warning of*
- > *such. The digital certificate does not identify the sender of the*
- > *message, only who signed or encrypted the BODY of the message. You could,*
- > *for example, sign a message and have it relayed from an anonymous*
- > *remitter. As long as that remailer never altered the BODY of the message*
- > *then its hash is still valid and unaltered and you, the one that signed*
- > *it, will still be correctly identified although the *header* show that it*
- > *came from the anonymous remailer instead of from your domain's mail*
- > *server.*
- >
- > *When you encrypt a disk to ship to someone, do YOU actually have to carry*
- > *it to the recipient? No. You encrypt it and then hire some shipper to*
- > *deliver it, and obviously the shipper wasn't you but that does not alter*
- > *the fact that YOU were the one that encrypted the disk. The certificate*
- > *says who signed or encrypted the BODY of the message. It does NOT qualify*
- > *or validate the sender of that signed or encrypted content.*
- >
- > --
- >
- > _____
- > *Post your replies to the newsgroup. Share with others.*
- > *E-mail reply: Remove "NIXTHIS" and add "#VS811" to Subject.*
- > _____
- >