

Re: Potential vulnerabilities of the Microsoft RVP-based Instant Messaging

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-03/0039.html>

From: Luke Kenneth Casson Leighton (lkcl@SAMBA-TNG.ORG)

Date: 03/21/02

Date: Thu, 21 Mar 2002 21:20:01 +0000
From: Luke Kenneth Casson Leighton <lkcl@SAMBA-TNG.ORG>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

On Thu, Mar 21, 2002 at 10:21:15AM +0200, Dimitrios Petropoulos wrote:

> *Russ/Greg,*

>

> > *Further to Greg's comments about this Encode Security Labs*

> > *analysis of MS Instant Messaging, a couple of things seem not*

> > *to be pointed out in the analysis.*

could someone please let the list know [not me, i'm out of the picture and don't have the time to investigate even if you did send it to me] if this "instant messaging" occurs over MSRPC, or if it occurs over some other protocol.

it's important to find out because if it's over MSRPC then you get all sorts of benefits that DCE/RPC provides, such as digital signing, etc. [if the good-old MS IM boys knew how to switch it on, that is].

if it's over some MS "home-brew" transport that just happens to use NTLM for authentication purposes 'cos the designers were told to then i'm not going to be the one to run a book on how many security flaws can be found in it, let's put it that way.

however, without having access to any resources whatsoever, my guess is that if it's part of exchange, then it's highly likely that DCE/RPC is involved, and therefore quite likely that DCE/RPC digital signing is also involved.

if that is the case, then all you'll need to do is to ensure that NTLMv2 is negotiated, and you'll be a lot better off.

only a packet trace / packet analysis will tell for sure.

NT-Bugtraq: Re: Potential vulnerabilities of the Microsoft RVP-based Instant Messaging

netmon should identify the traffic as MSRPC immediately, which is a big clue.

- > > *1. Exchange Server 2000 Instant Messaging supports the use of*
- > > *NTLM for authentication, as opposed to the Digest*
- > > *Authentication described and used in the analysis. The use of*
- > > *NTLM significantly alters the analysis, since it addresses*
- > > *man-in-the-middle attacks, unilateral authentication, and*
- > > *data origin authentication.*

the comments below initially refer to NTLMv1, i will do NTLMv2 later.

- >
- > *I may be mistaken but I don't think that NTLM authentication alters the*
- > *findings significantly. Here's why:*
- > *NTLM is a unilateral authentication protocol where the server*
- > *authenticates the client (the client receives the challenge from the*
- > *server, calculates the hash of the user's password*

the hashes are not calculated at this time, they are calculated when the account is created, and stored, for later use in the SAM database (on nt5 they are now stored in LDAP, using a method which has not been publicised by microsoft, so we don't know if it's secure or not).

this copy in the account database is used for verification purposes.

when a user logs on, the hashes are calculated from the cleartext password at the dialog box, and stored temporarily in memory, for future client-side usage, as you are describing, here.

- > *and uses this to*
- > *encrypt the challenge).*

the server uses the stored copy, and the client uses the cached copy.

both client and server perform the same response calculation, which is a DES-based algorithm and so is, these days, utterly pathetic as far as real security is concerned, using the challenge issued, as you say, by the server.

- > *The fact therefore remains that a malicious user*
- > *could masquerade as a server and convince the client to perform NTLM*
- > *authentication with the malicious user.*

NT–Bugtraq: Re: Potential vulnerabilities of the Microsoft RVP–based Instant Messaging

this is correct – if you are referring to NTLM challenge–response version 1. (NTLMv1).

in fact it's a very good way to farm user's passwords, as demonstrated by Paul Ashton back in 1996.

for example, you pre–calculate a database of simple challenges (e.g. 00 00 00 00 00 00 00 00) and the responses from a dictionary.

then you have a lookup table to go back from the response to the cleartext password.

it's also very easy to ask clients to "downgrade" to the weaker NTLMv1.

clients and servers are, at present, set to negotiate the highest common security level.

and if you are a malicious server that's easy to set to the lowest and most insecure level.

in the next few years microsoft will move over to setting the default setting to exclude NTLMv1.

this is standard "phase–out" policy that has to be offset against the number of users bitching at them on the phone and the internet and wasting their money over how "i upgraded and i can't log in anymore".

now, if you use NTLMv2, then this uses the following additional security features:

- NTLMv2 only uses the NT# not the weaker LM#.
- HMAC_MD5 is used, iirc, three times, which increases the computational complexity by a factor of approximately 50 (which makes brute force cracking 50 times more expensive than trying to crack an NTLMv1 NT#–based challenge, which is pretty expensive as it is)
- the CLIENT issues a random challenge to the server, along with a digital signature based on that AND the server's challenge.

this ensures that both the client AND the server know that they are not being spoofed.

- the challenge–response contains a timestamp, and if this timestamp is +/- 30 mins from the server's time, the server drops the connection.

NT–Bugtraq: Re: Potential vulnerabilities of the Microsoft RVP–based Instant Messaging

this is why you must now sync times correctly on NT5!

NOTE: the challenge–response, containing amongst other things, the timestamp, is digitally signed

– the challenge–response does NOT contain anything based directly on the NT#: instead, a hash of the NT# and the username AND the domain name AND the server challenge is used (HMAC_MD5(srv_chal, NT#+user+dom)) as a key which is then used AGAIN in HMAC_MD5 to calculate the digital signature of the challenge–response.

i think.

it's all been a long time ago, i'm not getting paid, it's a long story, this is all "free" advice, and it's irkesome to be giving "free" advice. so take it or leave it. grr :)

check the samba–tng source code if you want to analyse the algorithm. don't bother with samba.org source code: they don't understand what i did and it'll take them four years to get over their pride and another four years to work out the code, even with it staring at them in the face.

anyway. enough of that.

basically [despite having a 64–byte bottleneck even with 128–bit security negotiated and used for NTLMSSP encryption and digital signing], NTLMv2 is a heck of a lot better than NTLMv1 – a LOT better.

you won't be able to talk to w95 or NT4 SP3 and below or to AS/U or to AFPS you might be able to talk to PC–Netlink because the developer/porter talked to me and he thrashed out NTLMv2 properly into the code that AT & T and microsoft were supposed to have provided at NTLMv2 security level in the first damn place, but we don't care about w95 or NT4 SP3 and all the others, do we.

> *Furthermore, an initial NTLM authentication exchange does not offer any*
> *subsequent data origin authentication guarantees.*

no, it doesn't because NTLM is authentication, not encryption.

however, when you have a transport that uses NTLMSSP, then yes, you do have a few guarantees.

... but, due to security flaws in the NTLMSSP v1 algorithms (which use NTLMv1), you don't!

NT–Bugtraq: Re: Potential vulnerabilities of the Microsoft RVP–based Instant Messaging

... but, in NTLMSSP v2 (which uses NTLMv2), you do.

which is why, right at the top of this message, i asked if someone could find out if IM uses DCE/RPC (aka MSRPC) because DCE/RPC has the means to transparently provide NTLMSSP encryption and NTLMSSP digital signing.

and it is why i suspect that, if the IM boys home–brewed their own transport, i have a hunch that they didn't read the internal docs on how to use NTLMSSP, or what it even is.

- > *Two parties*
- > *communicating via IM –even if they have both successfully performed NTLM*
- > *authentication– do not share any common secrets or any other mechanism*
- > *in order to perform some data origin/integrity calculation (e.g. a*
- > *message authentication code or a digital signature). The fact therefore*
- > *remains that messages between two legitimate users could be altered in*
- > *transit and the recipient will not know that they have been tampered*
- > *with.*

that is why microsoft added SMB signing [to SMB, aka CIFS].

unfortunately it's quite computationally expensive (or it was in 1998) so people tend not to use it.

and it's also why NTLMSSP was invented.

and if it turns out that the boys who done IM actually used NTLMSSP, or if they used DCE/RPC, then the claims that you make, just above, are likely to be invalid.

if.

- > *Based on the two points above I think that man–in–the–middle attacks are*
- > *still possible even after NTLM authentication.*

man–in–the–middle attacks against the majority of microsoft protocols are relatively trivial to implement.

the main reason for this is because the majority of microsoft's services run over transport–independent layers [which provides all sorts of nice benefits both to developers and users].

e.g. NetBIOS is a transport that is now no longer implemented in its original form: instead, it is proxied over other transports, e.g. IPX/SPX and TCP/IP.

due to NetBIOS's origins as a LAN–only transport, it has no security built–in [but then again, neither does IPv4.].

NT-Bugtraq: Re: Potential vulnerabilities of the Microsoft RVP-based Instant Messaging

and due to the proxying *_also_* having no security built-in, it is very simple, as we know, to spoof NetBIOS.

sigh.

- > *Regarding the comparison of IM and SMTP security, I strongly agree: SMTP*
- > *does not offer any more security than IM. In the case of SMTP however,*
- > *the confidentiality and data origin of a message can be adequately*
- > *protected using S/MIME. This report is only pointing out that the IM*
- > *implementation under examination is lacking similar mechanisms.*

if someone were paying me money, i would do the analysis that would allow me to assess this.

as they're not, i have no time or resources available, so cannot.

sorry :)

- > *As I said before, I may be mistaken so I'd be grateful if any flaws in*
- > *the above reasoning could be pointed out to me.*

... there are very few people with a detailed understanding of NTLM and NTLMSSP.

it's a pretty disappointing area to be in.

even when you *_do_* tell microsoft that they have a security problem, and you can get them to understand it, they don't ask your advice on how to fix it, they just go ahead and release, 18 months later, an equally unreviewed and possibly broken "fix" that takes a further 12 to 18 months to work out and understand.

... of that group, a large number of them are encumbered by restrictive proprietary practices and agreements such that even if they knew what the problems were and had the source code staring at them in the face, they couldn't tell you anyway.

... so please forgive me for advising you to read the samba tng source code [grep for ntlmv2] smbencrypt.c, srv_pipe_ntlmssp.c and cli_pipe_ntlmssp.c, which has an implementation of ntlmv2, ntlmv1, ntlmssp1 (40-bit only) but does not have – yet – ntlmssp1 (128-bit) nor does it have ntlmssp2 [why? because i am not being paid to, that's why].

and also to the appendix B of my book, ISBN 1578701503 called "DCE/RPC over SMB: Samba and Windows NT Domain Internals", which contains outlines of the algorithms just mentioned above, amongst other things. available on amazon.com [shameless plug].

NT-Bugtraq: Re: Potential vulnerabilities of the Microsoft RVP-based Instant Messaging

regards,

luke

--

this message is private, confidential, and is intended for the specified recipients only. if you received, altered, deleted, modified, destroyed or interfered with the contents of this message, in whole or in part, please inform the sender (that's me), immediately.

if you, the recipient, reply to this message, and do not then receive a response, please consider your reply to have been lost or deliberately destroyed: i *always* acknowledge personal email received. please therefore take appropriate action to ensure effective communication.

thank you.

-
- ***Previous message:*** Richard M. Smith: "Questionable security policies in Outlook 2002"
 - ***In reply to:*** Dimitrios Petropoulos: "Re: Potential vulnerabilities of the Microsoft RVP-based Instant Messaging"
 - ***Next in thread:*** Brown, Keith: "Re: Potential vulnerabilities of the Microsoft RVP-based Instant Messaging"
 - ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]