

## Re: Remote Desktop MITM Concerns

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-06/0153.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 06/13/05

Date: Sun, 12 Jun 2005 22:13:57 -0500

I would not lose sleep if I were you. I still use TS accross the internet and don't worry about it. Since you are using an IP the threat is almost non existant as a user can not simply reconfigure their public IP to spoof you into connecting like they can a lan IP due to the way the internet is routed. Then always look at the worse case scenario as part of managing your risk. What would be the consequences if someone read your data? If it meant that people would die or be harmed, or a that customers credit card numbers could be obtained then you must use a l2tp VPN connection to mitigate the risk but my guess is that is not the case as hopefully you would already be doing such. --- Steve

"JerryTheGreat" <JerryTheGreat@discussions.microsoft.com> wrote in message news:F74D73A1-CC31-4A0C-B854-31ADD2912793@microsoft.com...

> *What I really want to know here is this: How significant a concern is this?*

> *If the ability to perform the act is integrated into freely available software should I be concerned? In my setup, I am logging in accross the Internet, so IPsec is out, unless I set up a vpn. Mitigating the risk is that*

> *I use IP, not DNS to connect to the server, which should make a MOTM extremely difficult to perform without detection.*

>

> *Thanks.*

>

> *JTG*

>

> *"Roger Abell" wrote:*

>

>> *I am with Steve in replying that, if you feel your environment of*

>> *sufficient*

>> *value that there actually is a risk someone would consider mounting an*  
>> *man*

>> *in the middle compromise of your network communications, then you should*

>> *look at use of a IPsec hard security association, in one or another form,*

>> *and then use RDP within this.*

>>

>> *The underlying problem here is that RD is intended to allow ad-hoc type*

>> *connections, such as with consumer stand-alones. When there is no third*

>> *party involved and there is no pre-shared secret, then it is*  
>> *fundamentally*  
>> *unavoidable that the types of mutual verification this author indicates*  
>> *as*  
>> *the most desirable are not infallibly possible.*  
>>  
>> --  
>> *Roger Abell*  
>> *Microsoft MVP (Windows Security)*  
>>  
>> *"JerryTheGreat" <JerryTheGreat@discussions.microsoft.com> wrote in*  
>> *message*  
>> *news:F875A484-5C95-44D8-8829-E2400FCFCAC1@microsoft.com...*  
>> > *Hello,*  
>> >  
>> > *Released May 28 was an unofficial security advisory entitled "Remote*  
>> > *Desktop*  
>> > *Protocol, the Good the Bad and the Ugly" By Massimiliano Montoro. This*  
>> > *has*  
>> > *me very concerned about my setup. Is this a valid issue?? I've found*  
>> > *no*  
>> > *advised from Microsoft or any other security site, except that the*  
>> > *nefarious tool Cain and Abel v2.7 contains this capability. Please*  
>> > *someone*  
>> > *address this concern for me.*  
>> >  
>> > *I'm being careful in this posting not to use any keywords a search*  
>> > *engine*  
>> > *may index.*  
>>  
>>  
>>