

RE: Windows Remote Desktop

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0219.html>

From: Depp, Dennis M. (*deppdm_at_ornl.gov*)

Date: 01/15/04

Date: Thu, 15 Jan 2004 13:29:26 -0500

To: Shawn Jackson <sjackson@horizonusa.com>, jamesworld@intelligencia.com

Two statements I don't agree with:

1) "Additionally no actual 'data' is transferred through the RDP connection, it's just interface information (mouse movement, button clicks, typing) and screen refreshes. Now if you were using the resource mapping then data would traverse the RDP connection and would be subject to its encryption."

Data is sent over the wire concerning keystrokes, mouse movements and screen refresh data. Obviously this information, particularly keystrokes can provide data to a hacker. However all information set via RDP is encrypted the default is 56-bit with the capacity to use 128-bit RC4. Even when using local resources, the data is still encrypted with 128-bit security.

2) "All in all I think that PCAnywhere and Citrix have more secure RDP/VNC like interfaces"

The default security setting in Citrix is basic (no encryption) PCAnywhere maybe better, I'm not sure. Both Citrix and RDP are vulnerable to MiM attacks. Citrix does have the capability to use SSL but this is comprable to Microsoft's VPN solution.

Denny

-----Original Message-----

From: Shawn Jackson [<mailto:sjackson@horizonusa.com>]

Sent: Wednesday, January 14, 2004 6:36 PM

To: jamesworld@intelligencia.com

Cc: Michael Gale; security-basics@securityfocus.com

Subject: RE: Windows Remote Desktop

Well transferring data outside a company is easier then pie these days. With everything from encrypted email to USB drives it's hard to use that as a sole point 'ban' RDP to offsite resources. Unless you're running at high level security i.e. Military, Extremely Sensitive Work, National Security the movement of data offsite would be a secondary concern.

SecurityFocus BASICS: RE: Windows Remote Desktop

The RDP encryption is 'in transit' protection and won't protect the resources. I personally never use the clipboard sharing, drive/printer mapping, etc. Access to those resources should be dictated by the company security policy and doesn't follow the 'security' of the protocol/connection. Seaming the connection is one-way (From Workstation or RDP Host) it hard to open a hole/exploit through an infected RDP host and use the RDP interface to your advantage.

Additionally no actual 'data' is transferred through the RDP connection, it's just interface informatio