Windows Remote Access

A newsletter for IT Professionals

I. Background of Remote Desktop for Windows

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that enables users to interface with another computer through a graphical interface. RDP is based on, and is an extension of, the T-120 family of protocol standards, which is a multichannel capable protocol allowing for separate virtual channels for carrying presentation data, serial device communication, licensing information, highly encrypted data (keyboard, mouse activity), etc.

RDP supports multipoint (multiparty sessions) data delivery, allowing data from an application to be delivered in "real-time" to multiple parties without having to send the same data to each session individually (for example, Virtual Whiteboards). Thus, RDP is designed to support different types of network topologies and multiple LAN protocols.

RDP listens on TCP port 3389 by default, and uses RSA Security's RC4 cipher, a stream cipher designed to efficiently encrypt small amounts of data to secure communications over networks. Beginning with Windows 2000, administrators can choose to encrypt data by using a 56 or 128-bit key.

Updated versions of RDP include new functions and enhancements:

- **Windows 2000:** Terminal Services includes enhanced RDP 5.0. The Terminal Services Advanced Client (TSAC) also supports the RDP 5.0 feature set. While continuing to provide excellent performance over the LAN, RDP 5.0 also provides enhanced performance over low-speed connections.

- **Windows XP:** Uses RDP 5.1 for Remote Desktop Connection and for Remote Assistant. Windows XP also includes Remote Desktop Web Connection, which is an updated version of TSAC (an RDP client based on a Microsoft ActiveX control). Remote Desktop Web Connection supports RDP 5.1 and RDP 5.0. Starting from RDP 5.1, new features are supported including Smart Card authentication, keyboard hooking (directing special Windows key combinations), and sound, drive, port, and network printer redirection. RDP 5.1 also has improved performance over low-speed dial-up connections through reduced bandwidth.

- **Windows Server 2003:** Uses RDP 5.2 for Remote Desktop Connection and for Remote Assistant. Remote Desktop Web Connection supports RDP 5.2 and is backward compatible with RDP 5.1 and 5.0. Major enhancement of RDP 5.2 includes the support of secured remote desktop connections using TLS/SSL based authentication.

Reference:
http://support.microsoft.com/?scid=kb;en-us;186607&x=6&y=10
http://msdn.microsoft.com/en-us/library/aa383015(VS.85).aspx

II. Risk of Remote Desktop in Universities

Continuous advancements have been made to improve Remote Desktop security; however, universities still remain as a major target for exploiting Remote Desktop vulnerabilities:

1 **Lack of security awareness** – Although today's user is more IT savvy, lack of security awareness is still one of the leading causes for RDP exploits. Remote access users must be made aware of their security responsibilities.

Awareness training and formally documented policies and procedures can help inform remote access users on important security topics. Such training and policies should include best practices to adhere to when working outside of the office, firewall configuration and password requirements.

2 **Local Administrative Right –** Most of the users are granted with local administrative right on their computers. With the administrative right, users have full control over the configuration and software installation of the computers.

In some cases, best practice of configuration may have been performed on local computers of users by IT department. However, since the local administrative right resides with the users, configurations can be easily modified or reset. Users who are not aware of the risks with using RDP access will be more susceptible to information disclosure attacks and brute force attacks.

3 **Use of 3rd party software –** Users may use 3rd party software readily available on the internet for remote desktop access such as EchoVNC, iTALC, rdesktop, RealVNC Free and TightVNC. There may be vulnerabilities present in these 3rd party softwares which may be exploited by the attacker. For instance, vulnerability has been reported for TightVNC in March 2009, which can be potentially exploited by a malicious hacker to compromise a target computer. User awareness education and regularly update the version and security patch can reduce the adverse effect by the vulnerabilities. This can also be secured by using the highest level of encryption which encrypts the data transmission in both directions by using a 128-bit key.

Reference:
http://www.sans.org/reading_room/whitepapers/terminal/secure_remote_access_using_windows_terminal_services_2003_1354

II. Risk of Remote Desktop in Universities (cont'd)

4 **Un-patched Operating Systems** – Un-patched Operating Systems leave vulnerabilities exposed and compromises overall security within the system. Windows Remote Desktop, in particular, has had a history of related patches to address several major vulnerabilities. For example, Microsoft released a security patch (MS09-044) in August 2009 to improve the security of Windows Remote Desktop. The patch helped fix a heap-based buffer overflow problem in Remote Desktop Connection that allowed attackers to execute arbitrary code via unspecified parameters.

Administrators should apply the latest patches as soon as possible to mitigate such risks. Patches should be tested on a test server first to avoid any problems or incompatibility issues with the new patch.

5 **Decentralised PC administration –** Due to the large number of students and staff who require remote access to work off-campus, it is difficult for universities to centrally manage the computers requiring remote access. Furthermore, it is not feasible for the IT department to configure each computer for secure remote desktop connection. As a result, universities are susceptible to greater risks as remote access users may have weak configurations or may be unaware to the security risks when using RDP. Computers with weak configuration may be compromised, and used by attackers to perform further attack within the university network.

Universities may consider limiting RDP access to only certain users (e.g. students for courses requiring remote access). Administrators can also consider restricting the range of IPs that can remotely connect to the server. This can be done by configuring the firewall to provide additional access control using user-based authentication or IP restrictions. Alternatively, server configuration can be hardened by using IPSec to filter IPs.

Reference:
http://www.sans.org/reading_room/whitepapers/terminal/secure_remote_access_using_windows_terminal_services_2003_1354

II. Risk of Remote Desktop in Universities (cont'd)

6 **External threats** – Based on the factors above, universities remain a prime target for external attackers to exploit Remote Desktop vulnerabilities. Below are some examples of attacks that can be performed on universities:

- ***Enumeration on server port –*** Enumeration is the process of gathering information about a target system or network a hacker wants to compromise. Identifying active Terminal Server ports is generally the first step in an attack. One method is to use an internet search engine such as Google to locate the ActiveX authentication form in the default location TSWeb/default.htm. Changing these default parameters and removing these common text strings from your installation can easily "hide" your connection page from this type of search.

  Another common method is to do a port scan for TCP port 3389, which is the default port for RDP. Once an open port is located, the attacker can use their Terminal Server client to connect to the target IP and be prompted for login and password. Hackers can then perform a Brute Force attack and gain access to that Terminal Server. To mitigate this risk, the port number should be changed to a non-standard port for both the Remote Desktop Connection & Remote Desktop Web Connection. Connecting to the Terminal Server using other methods such as VPN, RAS or SSL will also prevent external attacks using this method.

- ***Password Guessing Attacks*** – Password guessing is still the primary method for attacking Terminal Servers. Dictionary based password-cracking tools are available to guess passwords using brute force. It takes advantage of the fact that the Administrator account cannot be locked out for local logins and, therefore, can be cracked through unlimited attempts. This is all done through the encrypted channel, which may allow the attacker to go undetected by Intrusion Detection Systems.

  Important risk-mitigating controls include configuring low account lockout thresholds with manual reset, implementing complex passwords that are changed on a frequent basis, implementing a logon banner, disabling of shared accounts, and renaming the Administrator account. Connecting through a VPN or SSH tunnel, limiting access control by IP or other information, or using 2-factor authentication will add further protection against this threat.

- ***Local Privilege Escalation –*** The interactive rights required for Terminal Server access allows the ability to run privilege escalation and grant the attacker Administrator equivalent privileges. Attackers are utilising the zero-day vulnerabilities to launch blended exploits. This type of vulnerability allows for an interactively logged in user (either at the physical host or using some remote-desktop type of network application) to elevate their privileges to higher-privileged accounts, typically Administrator or SYSTEM. The attack tools are freely available for download on the Internet and other methods use only the tools available in a session. Access control lists and software restriction policies must be carefully designed to protect against this threat. Disabling Active Desktop also prevents a few specific attacks.

Reference:
http://www.sans.org/reading_room/whitepapers/terminal/secure_remote_access_using_windows_terminal_services_2003_1354

III. Exploitation on Remote Desktop

Vulnerabilities in Remote Desktop Connection

Vulnerabilities have been discovered in the Microsoft Remote Desktop Connection which could allow an attacker to take complete control of an affected system. Exploitation occurs if a user uses Microsoft Remote Desktop Connection to connect to a malicious RDP server, or if a user visits a web page or opens a malicious e-mail attachment which is specifically crafted to take advantage of these vulnerabilities.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

A recent vulnerability (MS09-044) has been discovered in Aug 2009 in the Microsoft Remote Desktop Connection that could allow an attacker to take complete control of an affected system.

- **Description of vulnerability –** The vulnerabilities could allow remote code execution if an attacker successfully convinced a user of Terminal Services to connect to a malicious RDP server or if a user visits a specially crafted web site that exploits this vulnerability.

- **Impact of vulnerability –** Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

- **Affected RDP versions –** Microsoft Terminal Services Client ActiveX control running RDP 6.1 on Windows XP SP2, Vista SP1 or SP2, or Server 2008 Gold or SP2; or 5.2 or 6.1 on Windows XP SP3.

- **Recommendation –** Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Reference:
http://www.msisac.org/advisories/2009/2009-052.cfm
http://www.microsoft.com/technet/security/bulletin/ms09-044.mspx

IV. Hardening steps to secure Remote Desktop access. (Basic Security Recommendations)

The following security recommendations or guidelines help secure your server:

1 **Rename the Administrator Account –** Renaming the Administrator Account will help to prevent a brute force attack on the Administrator account. Most brute force attacks will use the account name "Administrator". This is the default name and this account is not subject to account lockout. This configuration change is done by editing the Local Security Policy.

2 **Change the default RDP port –** For the attack surface exposure of the common RDP port (TCP 3389), the RDP session can be configured to use a different port. The modification must be applied to both the terminal server itself and all of the TS clients. Modification of registry will be required to change the default of the terminal server, and modification of the Client Connection Manager will be required to alter the port for client side. Please refer to http://support.microsoft.com/kb/187623 for details of configuration.

3 **Use the highest level of encryption –** Use the High encryption option which encrypts the data transmission in both directions by using a 128-bit key. Use this level when the Terminal Server runs in an environment that contains 128-bit clients. RDP traffic is encrypted using 128-bit encryption when connecting to Windows Server 2003 from a Windows XP client computer. By default, both the Web-based and the standalone remote desktop client send the encrypted RDP traffic over TCP port 3389.

4 **Set Group Policy settings for the remote desktops –**By making end users members of the Remote Desktop Users group you grant these users the necessary privileges for connecting to Terminal Server.

The Remote Desktop Users group allows the same access as the Users group with the additional ability to connect remotely. By using this group, you save administrative resources by not having to set up these rights for each user individually. By default, the permissions for a Terminal Server environment are set to provide maximum security while allowing users to run applications. Users can save files within their profile directory, but cannot delete, or modify certain files.

5 **Restrict users to specific programs –** Software restriction policies provide administrators with a policy-driven mechanism to identify software programs running on computers in a domain and to control the ability of those programs to execute. You can use policies to block malicious scripts, to lock down a computer, or to prevent unwanted applications from running.

Reference:
http://technet.microsoft.com/en-us/library/cc264467.aspx
http://download.microsoft.com/download/4/2/9/42995217-e85a-41e9-b530-375a10b800fa/TS_security.doc

Copyright Statement
All material in this document is, unless otherwise stated, the property of the Joint Universities Computer Centre ("JUCC"). Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

A single copy of the materials available through this document may be made, solely for personal, noncommercial use. Individuals must preserve any copyright or other notices contained in or associated with them. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the copyright holder of the materials. Contact information for requests for permission to reproduce or distribute materials available through this document are listed below:

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC),
Room 223, Run Run Shaw Building,
c/o Computer Centre, The University of Hong Kong,
Pokfulam Road, Hong Kong