



---

# Security Considerations for rdesktop and Windows Terminal Services

---

**Published by the Open Source Software Lab at Microsoft. March 2008.**

Special thanks to Chris Travers, Contributing Author to the Open Source Software Lab. Most current version will be maintained at <http://port25.technet.com>.



---

## **Abstract:**

Microsoft Terminal Services provides an important set of functionality for remote administration and centralized application management. This service allows administrators to log in remotely and with full access to the system. Similarly, users can log in and run specific applications, which are centrally managed by IT personnel.

---

Information in this document, including URL and other Internet Web site references, is subject to change without notice and is provided for informational purposes only. The entire risk of the use or results from the use of this document remains with the user, and Microsoft Corporation makes no warranties, either express or implied. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

© 2008 Microsoft Corporation. This work is licensed under the Microsoft Public License. The Microsoft Public License is [available here](#).

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft, Windows, Windows XP, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

---

## 1.1 Introduction

Microsoft Terminal Services provides an important set of functionality for remote administration and centralized application management. This service allows administrators to log in remotely and with full access to the system. Similarly, users can log in and run specific applications, which are centrally managed by IT personnel.

The most frequent client for this service is `mstsc.exe`. Although this ships with Windows, updated versions are available as free downloads from the Microsoft website. As of this writing, the most recent version, 6.0, is available at <http://support.microsoft.com/kb/925876>.

The standard client for Linux systems is `rdesktop` (source code available at <http://www.rdesktop.org>). As of this writing, the most recent version is 1.5.0. This version still offers support for RDP versions 4 and 5 (with only basic support for 6).

`Rdesktop` is shipped with many Linux distributions, and on Fedora Core 5, version 1.4.1 can be installed simply using the following command:

```
bash# yum install rdesktop
```

## 1.2 Basic use of Rdesktop

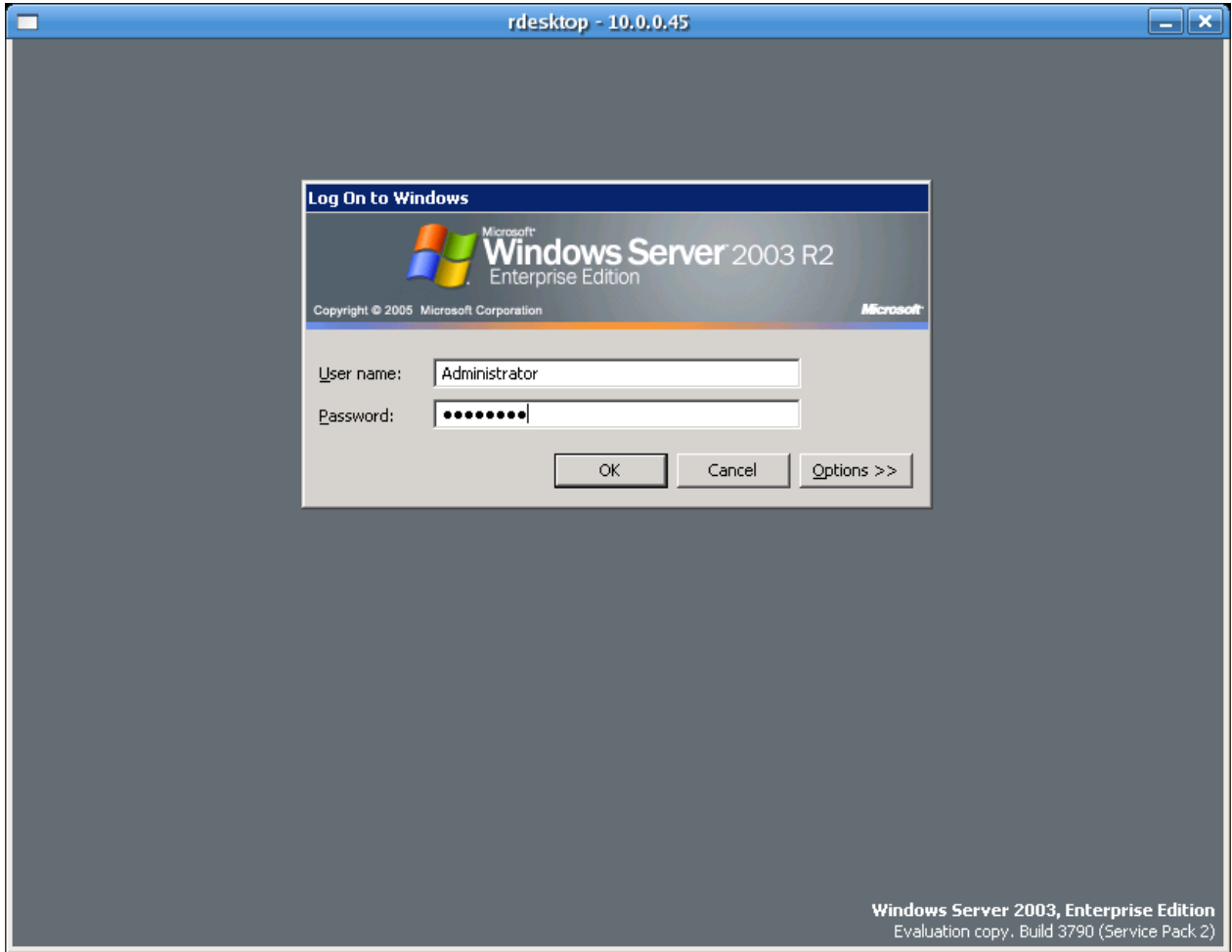
`Rdesktop` is a command-line tool and can be used to connect to a server using a command such as:

```
bash$ rdesktop -a 24 hostname
```

Commonly used options include:

- u username
- d domain
- p password (unsafe, see below)
- s shell (starts a specific application instead of explorer)
- a colordepth (i.e. 8, 16, 24)
- N (enables Numlock synchronization between the `rdesktop` session and the X server).
- P (Use a persistent cache of bitmaps)
- r device (redirect a specific device, such as a disk, printer, sound card, etc)

The following screenshot shows `rdesktop` on Linux connecting to a Windows Server 2003 R2 system.



### 1.3 -p Password is Considered Dangerous

Command-line options on Linux can be observed by other users of the system using the `ps` command or the `proc` filesystem. For this reason, specifying sensitive information, such as a password on the command line is generally considered a poor security practice. Note, however, that this specific problem only affects multi-user systems (using this option on a single-user desktop or laptop is likely to be reasonably safe).

A second issue in this choice affects this option in combination with others. For example, Rdesktop supports a little-known option (`-E`) which disables encryption of the initial login packet. The `-E` option is dangerous in itself, but does not prevent encryption on interactive logins. However, if it is used with the `-P` password option, any user of the network able to read traffic off the wire may be able to capture the password of the user.

### 1.4 Security Considerations for RDP v5

RDP v6 adds two new security enhancements that are not supported by any version of rdesktop as of the writing of this paper: Network Level Authentication and Terminal Service Gateways.

RDP does not appear to support Kerberos in any strong way, and is based on the OSI/ITU T.128 protocol. Essentially, this means that RDP is an extension of the same protocol that Netmeeting uses to share

applications. In general OSI protocols are built under very different assumptions than those which were designed exclusively for TCP/IP. For this reason, the security assumptions are different too. I am not aware of any OSI protocol which specifies Kerberos support, nor am I aware of any implementations which supports Kerberos.

Kerberos is used by Active Directory in areas other than Terminal Services to mutually authenticate clients and servers. In other words, the server is authenticated to the client just as the client is authenticated to the server. This arrangement prevents servers from being impersonated in order to gather authentication information of users or otherwise perform malicious activities.

RVP v6 adds an alternative to Kerberos called Network Level Authentication. This ensures that the server is authenticated to the client before the client is authenticated to the server. Details regarding how this is done are sparse, but appear to use the OSI/ITU X.509 public key infrastructure standard.

Without mutual authentication, it is possible that a malicious user could set up a terminal services lookalike which was configured to gather usernames and passwords from those who tried to log in or perform other malicious activity.

OSI protocols were originally developed to run over hybrid voice/data networks similar to a cross between the public switched telephone network (PSTN) and the internet. For this reason, single sign-on support is handled using a gateway in a similar manner to the way a telephone device might use an exchange, such as a PBX or the switch at the telco's central office.

RDP v6 adds support for such gateways. This is not supported on any version of rdesktop as of the writing of this paper. The lack of such support means that users must log in separately on every rdesktop session, or that the harmful -P password option might be used in connection scripts.

## **1.5 Final Thoughts**

Rdesktop does have a number of security concerns due to its lack of support for the advanced security features of RDP v6. Most of these concerns also affect older RDP servers running Windows 2000 Server and the like.

Most of these issues can be worked around to some extent. However, many of the solutions are neither elegant nor seamless. IT personnel should evaluate the risks and determine whether use of RDP in general, and rdesktop in particular, fall within the acceptable security risk threshold.

If they do not, then a number of other techniques may be employed to reduce the risk at the expense of more intrusive security and/or greater management overhead. For example, packets could be filtered out selectively via internal routers, SSH tunnels or other VPN technology could be required (since these generally provide mutual authentication), or the like.

## **1.6 About the Author**

Chris Travers is the owner of Metatron Technology Consulting, a firm devoted to helping businesses and individuals leverage open source software on any platform. He has experience in network and protocol security evaluation, platform support of Windows and Linux, software development, and has followed the rdesktop project for over three years.