PROTECT

Using Remote Desktop Clients

INTRODUCTION

1. Remote access solutions are increasingly being used to access sensitive or classified systems from homes and public places. One common method of enabling remote access is to use a remote desktop client.

2. This document provides guidance on security risks associated with the use of remote desktop clients. It is targeted at organisations using remote desktop clients to access Government and Protected systems over the Internet.

SECURELY CONFIGURING A REMOTE DESKTOP CLIENT

3. The following discusses some of the security risks associated with the configuration of remote desktop clients.

Copying files to mapped devices

4. Most remote desktop clients map local data interfaces for a host computer to a remote desktop session. This presents a security risk to an organisation as an adversary can transfer sensitive or classified information outside of a remote desktop session by attaching a USB storage device or writing to optical media.

5. Disabling the client drive mapping setting on a remote desktop server can reduce this security risk.

Virtual printing

6. The ability to access a virtual printer, such as a PDF or XPS printer, on a host computer, from within a remote desktop session, presents a security risk to an organisation. If a virtual printer is installed on a host computer, and virtual printing is enabled by a remote desktop client, an adversary can print from within a remote desktop session to a file on a host computer.

7. Disabling virtual printing for remote desktop clients can reduce this security risk.

Copy and paste

8. By default, a remote desktop client maps the clipboard within a remote desktop session to the clipboard of a host computer. While this performs a useful function it presents a security risk to an organisation. An adversary can use this

functionality to copy sensitive or classified information from within a remote desktop session and paste it into another document on a host computer.

9. Disabling the client clipboard mapping setting on a remote desktop server can reduce this security risk.

Disabling encryption after authentication

10. By default, a remote desktop client may disable the use of encryption once authentication of the client has been completed. This allows an adversary to eavesdrop on sensitive or classified information that is being communicated over a remote desktop session.

11. Ensuring encryption is enabled after authentication by a remote desktop client can reduce this security risk.

Weak encryption

12. A remote desktop client can offer varying degrees of encryption for protecting sensitive or classified information communicated between a remote desktop server and a remote desktop client. Often basic encryption in a remote desktop client is designed simply to obfuscate communications to protect against simple network capture rather than detailed cryptographic analysis.

13. If a remote desktop client does not implement DSD approved protocols and algorithms, using an encrypted tunnel that implements DSD approved protocols and algorithms will ensure that robust encryption is being used to protect sensitive or classified information communicated between a remote desktop server and a remote desktop client.

Single-factor authentication

14. A remote desktop client may only require the use of single-factor authentication to authenticate to an organisation's sensitive or classified system. An adversary with knowledge of a user's authentication credentials, such as their password, can gain unauthorised access to an organisation's sensitive or classified system, often until such time that a user changes their password. If unauthorised access is achieved remotely, it can be very difficult to detect or prevent.

15. Using multi-factor authentication, such as a password and a one-time randomly generated PIN, or a PKI certificate and password protected certificate store, can reduce this security risk.

PROTECTING INFORMATION IN A REMOTE DESKTOP SESSION

16. The following discusses some of the security risks associated with accessing sensitive or classified information during a remote desktop session.

Key logging

17. The ability to capture keystrokes on a host computer using a remote desktop client presents a security risk to an organisation. An adversary can remotely install key logging software to capture authentication information for a remote desktop session, or to capture sensitive or classified information entered during that session.

18. Using a trusted operating environment for a host computer can reduce the security risk of an adversary remotely installing key logging software.

Taking screenshots

19. The screenshot functionality of an operating system presents a security risk to an organisation. An adversary can exploit this functionality on a host computer through a number of methods, such as using the Print Screen key to copy sensitive or classified information to the clipboard, installing screen capture software, or installing malware, such as the Zeus bot, that detects the presence of a remote desktop session and automatically takes screen captures at pre-defined intervals.

20. The registry, or global keybindings, of a host computer can be modified such that the Print Screen key is unbound and performs no function. This will reduce the security risk of an adversary using the Print Screen key. In addition, an organisation can use a trusted operating environment for a host computer. This will reduce the security risk of an adversary installing screen capture software or malware.

Shoulder surfing

21. Using a remote desktop client to access an organisation's sensitive or classified system in a public location presents a security risk. This can allow an adversary, or curious bystander, to observe sensitive or classified information on the screen of a host computer.

22. Using extra care to reduce the chance of a host computer's screen being observed in public locations such as public transport, transit lounges and coffee shops can reduce this security risk. Using a remote desktop client in public locations should be avoided unless absolutely necessary.

Leaving a host computer unattended

23. Leaving a host computer unattended in a public location presents a number of security risks to an organisation. An adversary could use such an opportunity to steal the host computer, install key logging software or hardware, or if a remote desktop client has already authenticated to an organisation's system, gain access to sensitive or classified information.

24. Constant vigilance of a host computer when in use, and securing it appropriately when not in use, can reduce these security risks.

Access to information with heightened sensitivities

25. Allowing unrestricted access to an organisation's sensitive or classified system via a remote desktop client, particularly from a public location, presents a security risk to an organisation. An adversary that gains unauthorised access to an organisation's sensitive or classified system through a remote desktop client can cause greater damage if they have access to information and applications with heightened sensitivities.

26. Often a user of a remote desktop client will not need access to such information, particularly from a public location. Restricting access to only essential information and applications accessed via a remote desktop client can reduce this security risk.

Privileged access

27. Using privileged access via a remote desktop client, when accessing an organisation's sensitive or classified system, presents a security risk to the organisation. An adversary that gains access to a user's authentication credentials can cause greater damage should they have privileged access instead of unprivileged access. In addition, using these privileges remotely is much less likely to be detected.

28. Preventing the use of privileged access via a remote desktop client, including authenticating as an unprivileged user and then escalating privileges, can reduce this security risk.

PROTECTING ORGANISATION'S SYSTEMS

29. The following discusses some of the security risks associated with allowing a remote desktop session to connect to a sensitive or classified system.

Untrusted operating environment

30. A host computer used to access a sensitive or classified system via a remote desktop session has the potential to have been exposed to viruses, malware or other malicious code. This presents a security risk to an organisation as a host computer could inadvertently infect other computers on an organisation's sensitive or classified system, or be used to steal sensitive or classified information.

31. Key measures that an organisation can implement on a host computer to reduce this security risk include:

- using the latest version of the operating system and applications
- applying the latest security patches to the operating system and applications

- using application whitelisting to ensure only approved applications are run
- ensuring standard user accounts are used instead of administrator accounts
- using an anti-virus or Internet security product with up to date definition files
- using a personal firewall that provides both inbound and outbound traffic filtering
- removing all unapproved applications
- using strong passwords for user accounts that are changed on a regular basis
- segregating the host computer from the rest of the Internet for the duration of a remote session e.g. by using a virtual private network connection
- disabling routing between virtual private network interfaces and other network interfaces; and
- disabling Internet connection sharing.

32. Alternatively, instead of securing the operating system for a host computer, an organisation can provide a trusted operating environment via a Live CD or USB stick. Each time a remote desktop session is required, the Live CD or USB stick ensures that a trusted operating environment is used. Note that a host computer must be configured to boot from CD or USB for this method to work.

33. Additionally, with network access control, system administrators can set policies for system health requirements on a host computer used to access a sensitive or classified system via a remote desktop session. This can include a check that all operating system patches are up to date, an anti-virus program is installed and all signatures are up to date, and that a software firewall is installed and being used. Host computers that comply with all health requirements can be granted access while host computers that aren't healthy can be quarantined or granted limited access.

Residual information in a page file

34. Operating systems use a page file, also known as a swap file. A page file is a virtual extension of a host computer's memory which is stored on its hard drive. Sensitive or classified information accessed from a remote desktop client may be written to a page file throughout a remote desktop session. When a remote desktop session is completed, any sensitive or classified information that was written to a page file will remain until it is overwritten by the operating system. This presents a security risk to an organisation as an adversary may copy a page file and extract sensitive or classified information from it.

35. Configuring the operating system of a host computer to overwrite a page file at shutdown can reduce this security risk. Note this method is only partially effective for a host computer using a solid state drive. Alternatively, a host computer can implement full disk encryption or encrypt the page file (if using NTFS) to protect its contents.

Residual information in memory

36. A remote desktop client stores information in a host computer's memory during a remote desktop session. This information, if not properly sanitised after a remote desktop session is completed, can be captured by an adversary with physical access using what is known as a cold boot attack, potentially exposing sensitive or classified information.

37. Some remote desktop clients automatically scrub a host computer's memory after a remote desktop session is completed reducing this security risk. If automatic memory scrubbing is not implemented, to reduce this risk an organisation could implement one of the following processes.

- Ensuring that a user restarts their host computer at the completion of their remote desktop session. For this to be effective, quick boot must be disabled in in the host computer's BIOS.
- Ensuring that a user powers down a host computer for 10 minutes after they have completed their remote desktop session.

Sleep and hibernate functionality

38. Operating systems offer sleep and hibernate modes as part of their power saving functionality. This functionality allows the contents of memory to be retained or written to disk while the rest of a host computer is powered down. This presents a security risk to an organisation as sensitive or classified information stored in memory or on disk can be captured by an adversary with physical access to a host computer.

39. Disabling sleep and hibernate power saving functionality in the operating system of a host computer can reduce this security risk.

CONTACT DETAILS

40. Australian government agencies seeking clarification about this document can contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or assist@dsd.gov.au.