Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Using remote desktop clients

First published: December 2011
Last updated: October 2021

Introduction

Remote access solutions are increasingly being used to access organisations' systems and data. One common method of enabling remote access is to use a remote desktop client. This publication provides guidance on security risks associated with the use of remote desktop clients.

Securely configuring a remote desktop client

The following discusses security risks associated with the use of remote desktop clients.

Copying files to mapped devices

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

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

Virtual printing

The ability to access a virtual printer, such as a PDF 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, malicious actors can print from within a remote desktop session to a file on a host computer.

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

Copy and paste

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. Malicious actors can use this functionality to copy data from within a remote desktop session and paste it into another document on a host computer.

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

Disabling encryption after authentication

By default, a remote desktop client may disable the use of encryption once authentication of the client has been completed. This allows malicious actors to eavesdrop on data that is being communicated over a remote desktop session.

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

Weak encryption

A remote desktop client can offer varying degrees of encryption for protecting data 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.

If a remote desktop client does not implement Australian Signals Directorate (ASD)-approved protocols and algorithms, using an encrypted tunnel that implements ASD-approved protocols and algorithms will ensure that robust encryption is being used to protect data communicated between a remote desktop server and a remote desktop client.

Single-factor authentication

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

Using multi-factor authentication, such as a passphrase and a one-time randomly-generated PIN from a hardware token, can reduce this security risk.

Protecting data in a remote desktop session

The following discusses some of the security risks associated with accessing data during a remote desktop session.

Keystroke logging

The ability to capture keystrokes on a host computer using a remote desktop client presents a security risk to an organisation. Malicious actors can remotely install keylogger software to capture authentication data for a remote desktop session, or to capture data entered during that session.

Using a trusted operating environment for a host computer can reduce the security risk of malicious actors remotely installing keylogger software.

Taking screenshots

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

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 malicious actors 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 malicious actors installing screen capture software or malware.

Shoulder surfing

Using a remote desktop client to access an organisation's system in a public location presents a security risk to an organisation. This can allow malicious actors, or curious bystanders, to observe the screen of a host computer.

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

Leaving a host computer unattended in a public location presents a number of security risks to an organisation. Malicious actors could use such an opportunity to steal the host computer, install keylogger software or hardware, or if a remote desktop client has already authenticated to an organisation's system, gain access to data.

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

Access to data with heightened sensitivities

Allowing unrestricted access to an organisation's system via a remote desktop client, particularly from a public location, presents a security risk to an organisation. Malicious actors that gain unauthorised access to an organisation's system through a remote desktop client can cause greater damage if they have access to data and applications with heightened sensitivities.

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

Privileged access

Using privileged access via a remote desktop client, when accessing an organisation's system, presents a security risk to the organisation. Malicious actors that gain 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.

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

Protecting organisation's systems

The following discusses some of the security risks associated with allowing a remote desktop session to connect to an organisation's system.

Untrusted operating environment

A host computer used to access an organisation's 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 system, or be used to steal data.

Key measures that an organisation can implement on a host computer to reduce this security risk, or request an owner of a personally-owned device implement, include:

- using application control to ensure only approved applications are run
- using the latest version of an operating system and applications
- applying the latest security patches to an operating system and applications
- enabling security functionality in applications while disabling any unnecessary functionality
- ensuring standard user accounts are used instead of administrator accounts
- implementing multi-factor authentication where possible.

Additionally, with network access control, system administrators can set policies for system health requirements on a host computer used to access a system via a remote desktop session. This can include a check that all operating system patches are up-to-date, an antivirus or security product 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 data in a page file

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. Data 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 data 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 malicious actors may copy a page file and extract data from it.

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 data in memory

A remote desktop client stores data in a host computer's memory during a remote desktop session. This data, if not properly sanitised after a remote desktop session is completed, can be captured by malicious actors with physical access using what is known as a 'cold boot attack'.

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 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

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 data stored in memory or on disk can be captured by malicious actors with physical access to a host computer.

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

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate