



**NISCC Technical Note 04/03**

**Issued 27 June 2003**

## **Securing VNC (Virtual Network Computing)**

### **Key Points**

- Virtual Network Computing (VNC) is a commonly used Graphical remote access software application.
- Although the software has serious flaws, in the event that there is a business need for VNC, there are ways of minimising exposure to those risks by suitable configuration of the product.
- This technical note identifies the security flaws and provides configuration guidance.

**National Infrastructure  
Security Co-Ordination Centre**  
PO Box 832  
London, SW1P 1BG

Tel: 020 7821 1330 Ext 4511  
Fax: 020 7821 1686  
Email: [enquiries@nisc.gov.uk](mailto:enquiries@nisc.gov.uk)  
Web: [www.nisc.gov.uk](http://www.nisc.gov.uk)

## **Background**

1. Virtual Network Computing (VNC) is a freely distributed product from the AT&T laboratories in Cambridge (available from <http://www.uk.research.att.com/vnc>) that enables the remote viewing and control of a remote computer's desktop over a reliable network connection.
2. The software is freely available under the terms of the GNU public licence and has been ported to a wide range of operating systems, including all Microsoft Windows win32 platforms, most versions of Unix and even personal digital assistants thus extending its functionality to wireless devices.
3. This technical note aims to examine the security issues encountered with deploying VNC and where possible to make recommendations on how these issues can be overcome. The note will cover the official versions from the AT&T web site for Microsoft Windows (VNC version 3.3.3r9) and Solaris / Linux (VNC version 3.3.3r2). The intended audience of this technical note is administrators of systems that use VNC as a component product.
4. VNC has a number of serious security issues. It needs to be stressed that VNC does not provide security for sensitive information. Nevertheless, where a business case justifies the use of VNC, steps should be taken to secure the default installation. This technical note aims to provide guidance on how some of the risks can be reduced. The use of the information within this document does not guarantee a secure deployment of the product.

## **Software Components**

5. The software is distributed in two parts. The first is the server that sits on the host machine, and the second part is a client that connects to the server and allows the user of the client software to view the desktop of the remote system. The client can either be a standalone application or a Java application executed by using a web browser to connect to a simple web server that is part of the VNC server application.
6. By default the server listens on port (5900 + the display number) and the web server listens on port (5800 + the display number).

### **VNC Server for Microsoft Windows**

7. The Windows server can be run as either a true service or as a user level application. The server stores its configuration in the registry under the HKEY\_LOCAL\_MACHINE\ORL\WinVNC3 branch.

### **VNC Server for X**

8. The Solaris/Linux version of the server runs as a user level application that enables the remote viewing of an X-Window session. The user is required to log onto the machine using other means and then to start the VNC session.

### **VNC Web Server**

9. The VNC server also has a web server component that allows a web browser to connect to the server. This enables the browser to download a Java client that can be used to view and/or control the server.

## RFB Protocol

10. VNC uses the RFB (Remote Frame Buffer) Protocol developed by the AT&T Laboratories as the basis for VNC communications between the server and the client. The protocol does not specify any protection for data passing between the client and server and as can be seen from the trace below, the phrase “This is a test” can be easily seen as it is typed into the client and relayed to the server. Two packets are seen for each keystroke, one informing the server that a key has been pressed and the second showing that the key has been released.

000001F4	04	01	40	00	00	00	00	54	..@....T
00000206	04	00	40	00	00	00	00	54	..@....T
00000344	04	01	40	00	00	00	00	68	..@....h
0000034C	04	00	40	00	00	00	00	68	..@....h
00000368	04	01	40	00	00	00	00	69	..@....i
0000037A	04	00	40	00	00	00	00	69	..@....i
00000382	04	01	40	00	00	00	00	73	..@....s
0000038A	04	00	40	00	00	00	00	73	..@....s
0000039C	04	01	40	00	00	00	00	20	..@....
000003A4	04	00	40	00	00	00	00	20	..@....
000003D4	04	01	40	00	00	00	00	69	..@....i
000003DC	04	00	40	00	00	00	00	69	..@....i
000003E4	04	01	40	00	00	00	00	73	..@....s
000003F6	04	00	40	00	00	00	00	73	..@....s
000003FE	04	01	40	00	00	00	00	20	..@....
00000406	04	00	40	00	00	00	00	20	..@....
00000418	04	01	40	00	00	00	00	61	..@....a
00000420	04	00	40	00	00	00	00	61	..@....a
0000043A	04	00	40	00	00	00	00	20	..@....
00000474	04	01	40	00	00	00	00	74	..@....t
00000486	04	01	40	00	00	00	00	65	..@....e
0000048E	04	00	40	00	00	00	00	74	..@....t
00000496	04	00	40	00	00	00	00	65	..@....e
000004A8	04	01	40	00	00	00	00	73	..@....s
000004B0	04	00	40	00	00	00	00	73	..@....s
000004B8	04	01	40	00	00	00	00	74	..@....t
000004E8	04	00	40	00	00	00	00	74	..@....t

11. The display updates are sent to the client in a compressed but unencrypted form and although at the time of writing there are no known tools for sniffing and displaying this traffic, should someone have a desire to view such traffic it would not be difficult to develop an application to provide such a function.

## Authentication

12. To perform authentication between a VNC server and client a challenge response methodology is used. This involves the server sending a random challenge to the client. The client then uses a user supplied password as a key to DES encrypt the challenge and send it back to the server.

13. If the server can decrypt and verify the challenge using the server’s copy of the password the client connection is accepted.

14. The password sub-section of VNC does not have any mechanisms for enforcing a password policy. As a result a user can specify a weak password that could easily be guessed by a potential attacker.

15. The password is stored locally on the server and is DES encrypted. However the password is encrypted using a fixed key. Tools are readily available for decrypting the stored password.

16. Early versions of VNC have no means of limiting the number of failed logon attempts to a server. Consequently an attacker could attempt to gain access to a server by performing a brute force attack against the password. The latest release of VNC attempts to address this issue by limiting the number of failed logon attempts from a single IP address within a specified time frame. Whilst this does not prevent a brute force attack, it does extend the time it would take to perform such an attack.

## **Logging**

17. The level of logging available varies depending on the version of the server used. The Microsoft Windows win32 version has no logging while the Unix version has a limited logging capability. Unfortunately the log is stored in the home directory of the user running the server, which makes centralised log analysis difficult as a number of log files need to be checked and cross-referenced to identify any hacking attempt. The log file is also overwritten each time the server is started, causing potentially crucial information to be erased.

18. In addition, as the logs are created with the user ID of the currently logged on user, compromising the VNC server enables the attacker to view, modify or delete the logs.

## **Hardening the standard VNC installation**

19. There are a number of steps that can be taken to harden the default installation of VNC.

### **Preventing Unauthorised Configuration Changes**

20. By default, WinVNC stores its configuration in the registry under HKEY\_LOCAL\_MACHINE\ORL\WinVNC3. By default all users are granted modify rights to this branch. This should be changed so that only the administrator can make changes to the registry entries. This would prevent a user from making changes that could further weaken system security.

21. Under Unix the configuration is stored in the .vnc directory under the user's home directory. By default a user can modify these files. It is suggested that the file permission is changed to prevent a user from modifying his or her configuration.

### **Protecting Communications**

22. As has already been seen, the communications between the client and server are not protected. This can be overcome by tunnelling the VNC session over a more secure protocol. This could be achieved by the use of virtual private networks (VPNs), SSH or SSL. A patch is available that enables VNC to use SSL, and a detailed paper explaining how to secure VNC using SSH is available from the AT&T web site, <http://www.uk.research.att.com/vnc/sshwin.html>.

### **Limit Connections**

23. Under Microsoft Windows the registry key AuthHosts can be used to limit the range of IP addresses that can connect to the server. When used with the QuerySetting option, this enables you to limit which client machines can connect to the server. Under Unix the same functionality can be achieved through the use of TCP Wrappers, see [www.uk.research.att.com](http://www.uk.research.att.com).

## Correctly Handle Multiple Connections

24. In a default installation a server only allows a single client to be connected to the server at any one time. However, the behaviour of the server can be modified when a second user client attempts to connect. There are three possible connection modes: the first mode kills the original session and allows the second client to connect (which is the default state); the second mode allows all connections to stay connected; and the third mode denies all new connections whilst a session is currently in progress. The ConnectPriority value is used to define which behaviour should be adopted. Use of the third mode is recommended to prevent a denial of service attack being performed against a running session.

25. The Unix server can be configured to handle additional connections in a similar manner. To do so the user needs to specify the `--nevershared` and `--dontdisconnect` options when starting the server.

## Close All Inactive Sessions

26. To ensure that a user is not left logged on unnecessarily, it is recommended that under Windows the LockSetting value is set so that a user is logged off when disconnecting from the server. Under UNIX, the server should be set to die when a client disconnects.

27. The use of the `--to` option and `xxx` key enables you to specify a timeout that kills a session should it remain idle for a predetermined time. This is recommended as it reduces the chance of a session being hijacked.

## Conclusion

28. There are numerous business benefits to using VNC for access to remote systems, but there are also a number of risks that need to be managed. In particular, potential procurers of VNC need to be aware that VNC does not provide security for sensitive information.

29. The default installation of VNC is inherently insecure and, as such, has the potential to significantly degrade a system's overall level of security. Consequently it is essential that the business benefits be deemed to justify the additional risks introduced by installing VNC onto critical servers.

30. As has been described in this document, a VNC installation can be hardened, but even if this is undertaken there are still some issues that need to be addressed and evaluated in any risk assessment.

31. The sessions are unencrypted as they pass across the local area network, and reading the traffic is a trivial task. It is strongly recommended that sessions are tunnelled through a more secure protocol to prevent such an attack.

32. Even though passwords are used to protect the server, there is no way of enforcing a password scheme. It is recommended that users are educated on the need to use strong passwords and that the passwords are changed frequently. To enforce a password policy would require that the passwords are audited frequently using any of the freely available tools.

33. As the lack of logging under the Microsoft Windows win32 environment is of great concern, the use of a third party application to monitor and record network connections is encouraged wherever possible.

34. The Unix logging capability is weakened by the way VNC saves logs in the user's home directory. If possible a script should be deployed that, upon server termination, copies all user VNC logs to a secure central location for storage and analysis.

35. As with most software, there are bugs and vulnerabilities in VNC that have been discovered by the security community. As a result of this, it is vital that relevant sites (such as <http://www.uk.research.att.com/vnc>) are monitored to ensure that the most up to date version is used.