Name: Perry Déraps

VNC - A Call Centre Perspective

Introduction

This paper will describe the issues and policies required to reduce the security risk when our organization's call centre decided to use VNC as a remote control program to connect and perform tasks to their client's workstations.

Description

To be able to develop an effective security policy, you must first know about the software package and how it works. VNC is the acronym for Virtual Network Computing. VNC is a

remote display system that can work from many different platforms and from many different operating systems. In other words, VNC provides a universal, cross-platform virtual desktop. For example, you can remote view a UNIX machine from a Win95 computer or use a MacIntosh computer to view a Windows NT workstation. You may view any computer off your network or from anywhere on the Internet.

Olivetti Research Laboratory was the first to develop VNC which was acquired by AT&T in 1999. AT&T Laboratories Cambridge was created and continues the work on VNC. VNC is a thin client consisting of two components: server and viewer. The server component generates a

display of the desktop environment and the viewer component draws the display on the screen.

The protocol that VNC uses to connect a computer with the server component to a computer

with the viewer component is simple, open and platform independent.

There are many advantages to using VNC over other remote control programs:

- •No state is stored at the viewer. You could close your viewer in the middle of a command line and launch the viewer from a different machine and pick up exactly where you left off.

- •The viewer component is very small and can be run directly from a floppy. No installation is required. For example, the Win32 viewer is approximately a 150K in size.

- •It is shareable, so that one desktop can be displayed by several viewers.

- •It is freeware which means that you can download it, use it, redistribute it under the terms of the GNU Public License. Both binaries and source codes are available. In fact, many contributors have developed server and viewer components to a variety of different platforms.

- •The protocol will work over any reliable transport such as TCP/IP.

- •You can remote view a desktop via the internet with a java-enabled web browser. The server listens to http connections on port 5800 + display number (on window machines the display number is 0)

Setup

Download the appropriate file according to the type of platform used, from the following URL address:

http://www.uk.research.att.com/vnc/download.html

For this paper we'll concentrate on the windows version of VNC or WinVNC since a majority of the call centres serve a clientele comprised of Win9x/WinNT computers (as of this writing the version of WinVNC is 3.3.3r7).

For VNC to be useful to a call centre, the server component must be installed on all of the clients

workstations. The WinVNC service must be installed so that the server component will run automatically every time the client's workstation boots-up. Please note that when the service is installed, it will ask for a password. If none is given, WinVNC will not run.

The call centre only requires the viewer component. It is contained on one file labled vncviewer.exe which is small enough to carry on a floppy. The current VNC software requires a TCP/IP connection between the server and the viewer. To connect, run vncviewer.exe and type in the IP of the desired workstation. The server will ask for the password before allowing any connection to take place. Once established, you can now remote control the client's workstation. To disconnect, just close the VNC session.

Even though a password is required to establish connection, it must be noted that once you are

connected, the traffic between the viewer and server is unencrypted and could therefore be vulnerable to a sniffer. It is recommended to tunnel the session using some type of secure channel (ie: VPN, SSL, SSH)

Security Policy

The ability of being able to view and control clients workstations poses a security risk. We can reduce the risk by introducing the following policies:

1) Authorized use

Only the call centre staff are authorized to receive and use the viewer component of VNC. The clients workstations will only receive the server component of VNC, not the viewer (ie: delete vncviewer.exe from the client's workstation). The call centre staff could only remote connect to the workstation if they were in phone contact with the client. The VNC source code was modified to include a popup window in order for the client to give permission before connection could take place. This policy ensured that no connection would take place without the presence and permission of the client.

2) Password

In the case of a call centre, it is most likely that all the clients will contain the same VNC server password. Therefore, it is important to establish a strong password schema. The password should be 8 characters in length and comprised of a non-dictionary word with at least one upper case letter and a number. Passwords should be changed at a regular interval (ie: once every 3 months) or immediately upon a change in staff at the call centre. All the clients server passwords could be changed using a push technology such as ZEN.

3) Network servers

Do not allow the installation of the server component of VNC to any administrative accounts on the network. Limit the installations to only regular users.

4) Internet

Only allow server and viewer connection with a java-enabled web browser via the internet if the connection can be secured using acceptable encryption tunnelling such as a VPN to prevent snooping or hijacking of the connection. If this is not possible, then the java version of the viewer should not be used.

Conclusion

VNC can be a powerful tool for call centre staff in performing desktop support to their clients. Effective policy and auditing to enforce it will help in reducing the risk that remote display software can introduce to an organization's network infrastructure.

References

Author unknown, AT&T Laboratories Cambridge, Main Home page for VNC.

URL: http://www.uk.research.att.com/vnc/

Richardson Tristan, Stafford-Fraser Quentin, Wood Kenneth R., Hopper Andy "Virtual Network Computing", IEEE Internet Computing, Volume 2, Number 1, January/February 1998.

Laird Cameron, Soraiz Kathryn, "VNC works miracles for system administrators", August 1999.

URL: http://www.sunworld.com/sunworldonline/swol-08-1999/swol-08-vnc.htm

Tarbouriech Georges, "Virtual Network Computing, as known as VNC" , July 2000.

URL: http://www.linuxfocus.org/English/July2000/article155.shtm

Author unknown, SecurityFocus.com Bugtraq website, "VNC Server Weak Password Encryption Vulnerability", November 10, 2000. URL: http://www.securityfocus.com/bid/854