Virtual Network Computing: A Case Study

Yogesh Sonawane[1] Swati Desale[2] Mahesh A. Marathe[3]
[1,2]Student [3]Assistant Professor
[1,2,3]Department of Mechanical Engineering
[1,2,3]SSBT`s COET, Bambhori, Jalgaon, (M. S.), India

Abstract— Virtual Network Computing abbreviated as V.N.C. is a stupendous technology adverted for remote desktop sharing. It is an intelligible protocol, based on a graphic primitive. This efficacious application is mainly contemplated for triggering and con- trolling remote desktop with in a network. This protocol is intrinsically used for prospecting Graphical User Interface desktops on remote machines within a LAN or over a WAN and providing access to home computing environments. Usually applications on a network can be accessed and executed by users as per the permissions ascribed by the administrator but impotent to access the desktop. The "VNC" is one such application that helps in catering the imperative facilities for inducing specific applications on a remote machine. The ingenuousness and candor makes this protocol competent, robust and puissant. The VNC protocol is utterly independent of operating system, windowing system, and applications dissonant from other remote display protocols such as the Windows System and Citrix's ICA. The VNC server is used for sharing and dispensing its screen whereas the VNC client ganders and collaborates with the server.

Key words: Virtual Network Computing

I. INTRODUCTION

These things and much more can be done with a nifty little freeware utility called Virtual Network Computing, or VNC. VNC allows you to control one computer from another. It comes in 2 parts, VNC server, which runs on the computer you want to control and VNC viewer, which runs on the computer you are sitting in front of. Both parts will run on macs, PCs and Silicon graphics.

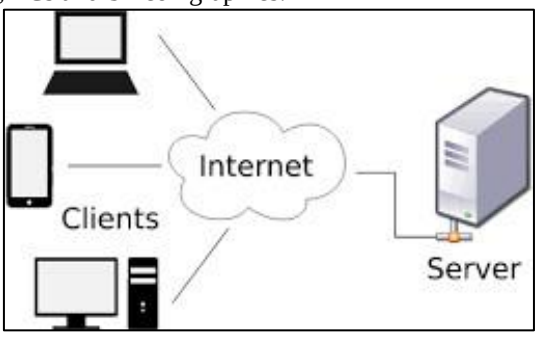

Fig. 1.1: Virtual Network Computing

It enables a remote user (who knows the password) to take control of your machine via the internet. They can view files, run programs, delete stuff, etc. In other words, they can use your computer exactly as if they were sitting in front of it, although a bit slower. This might sound a little frightening, and it is, except that you have a good deal of control over the situation. You set the password, you can kick them out if they abuse it, and you have to be online already and have VNC Server running for anyone to access your machine. In reality, you usually be setting up sessions specifically, or acting as the remote user yourself. Another nifty thing you can do with VNC is letting someone else watch your screen, but disabling their control over your computer. The best part about this is that they don't need anything special just a Java-capable web browser. VNC began its life at the Olivetti and Oracle Research Laboratory (ORL) as there. Teleporting System - this allowed the interface of an X Windows application to be displayed on a remote machine. However, this had relatively heavy resource and bandwidth requirements, plus the X security model was an issue. In 1994 the Video tile was built by ORL - this was a display device with Pen, LCD screen and ATM connection. The VNC Protocol was developed from the Videotile, utilizing the method of only transmitting the parts of the screen that changed, so greatly reducing bandwidth. In 1995 the Videotile mechanism was implemented in Java, so allowing anyone with a Java- equipped Web browser to access remote desktops running the relevant server software. It was now possible to access remote desktops from anywhere in the world, so providingfar greater flexibility.

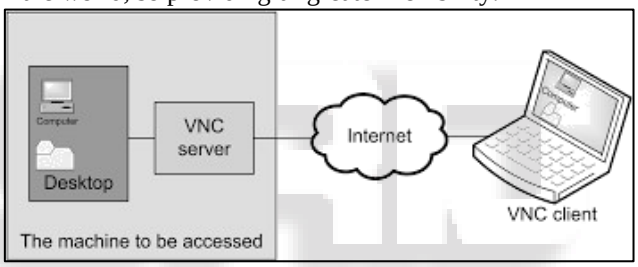

Fig. 1.2: Virtual Network

Virtual network computing (V.N.C) is a process of controlling a computer by sitting kilometers away through internet. Here we can control a server computer, which is situated kilometers away by sitting in front of a viewer computer. An image of the desktop of the server is brought to our computer and making events in viewer computer we can any work in the server computer. Here internet is used as the communication between the server and the viewer computer. As the operating system is graphical user interface the controlling is made by mouse events. When we brought the server desktop to viewer computer the screen resolution of the server and viewers must be same (eg: 800*600). This gives the protocol an adaptive quality: the slower the client and the network, the lower the rate of updates. This gives the protocol an adaptive quality: the slower the client and the network, the lower the rate of updates. The V.N.C technique has got a good future in the world of computer communication. Remote display system to view a computer from anywhere on the Internet and from a wide variety of machine architectures. A colorful or patterned desktop background will probably slow down VNC more than any other single factor. We have some suggestions on speeding up the twm window manager some Of which will also apply to other environments. It is a remote display system which allows you to view a computing desktop environment not only on the machine where it is running, but from anywhere

on the Internet and from a wide variety of machine architectures. Server sends small rectangles of the frame buffer to the client.

II. LITERATURE SURVEY

The Olivetti and Oracle Research Lab (ORL) at Cambridge in the UK developed VNC at a time when Olivetti and Oracle Corporation owned the lab. In 1999 AT and T acquired the lab, and in 2002 closed down the lab's research efforts. Developers who worked on VNC while still at the AT and T Research Lab include:

- Tristan Richardson (inventor)
- Andy Harter (project leader)
- Quentin Stafford-Fraser
- James Weatherall
- Andy Hopper

Following the closure of ORL in 2002, several members of the development team (including Richardson, Harter, Weatherall and Hopper) formed RealVNC in order to continue working on open-source and commercial VNC software under that name.

A. RFB Protocol

RFB (remote frame buffer) is an open simple protocol for remote access to graphical user interfaces. Because it works at the frame buffer level it is applicable to all windowing systems and applications, including Microsoft Windows, mac OS and the X Window System. RFB is the protocol used in Virtual Network Computing (VNC) and its derivatives. The VNC protocol expresses mouse button state in a single byte, as binary up/down. This limits the number of mouse buttons to eight (effectively 7 given convention of but- ton 0 meaning disabled). Many modern mice enumerate 9 or more buttons, leading to forward/back buttons having no effect over RFB.

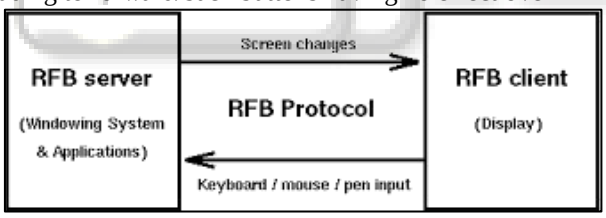

Fig. 2.1: RFB Protocol

B. Data Encryption Standard

The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Although now considered insecure, it was highly influential in the advancement of modern cryptography. DES is now considered to be insecure for many applications. This is mainly due to the 56-bit key size being too small. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (see chronology).

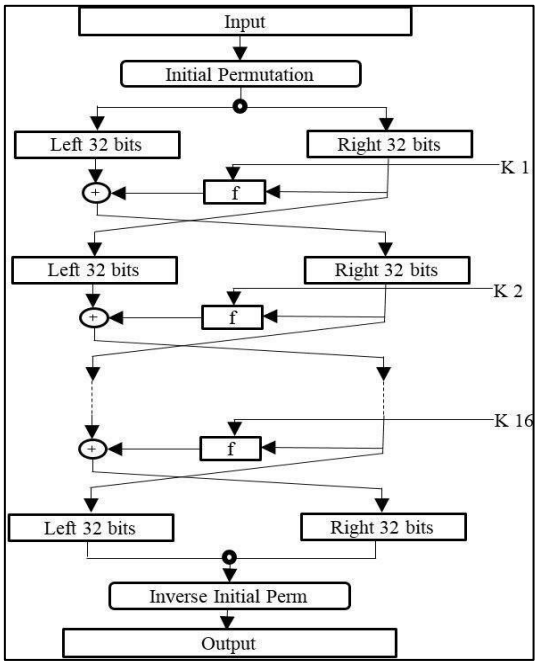

Fig. 2.2: Data Encryption Standard Process

One bit in each 8-bit byte of the KEY may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16,..., 64 are for use in ensuring that each byte is of odd parity. Like other block ciphers, DES by itself is not a secure means of encryption, but must instead be used in a mode of operation. FIPS-81 specifies several modes for use with DES. Further comments on the usage of DES are contained in FIPS-74.Decryption uses the same structure as encryption, but with the keys used in reverse order.

III. METHODOLOGY

A. General Methodology for VNC

In the normal method of operation a viewer connects to a port on the server (default port: 5900). Alternatively (depending on the implementation) a browser can connect to the server (default port: 5800). And a server can connect to a viewer in "listening mode" on port 5500. One advantage of listening mode is that the server site does not have to configure its firewall to allow access on port 5900 (or 5800); the duty is on the viewer, which is useful if the server site has no computer expertise and the viewer user is more knowledgeable. On Unix/Linux computers that support multiple simultaneous X11 sessions, VNC may be set to serve a particular existing X11 session, or to start one of its own. It is also possible to run multiple VNC sessions from the same computer. On Microsoft Windows the VNC session served is always the current user session [1].

B. Connection SetUp & Shutdown

To establish a client-server connection, the server first requests authentication from the client, using a challenge-response VNC server VNC viewer (client) VNC protocol scheme; the client typically requires the user to enter a password at this point. The server and client then ex- change messages to negotiate desktop size, pixel format, and encoding schemes. The client requests an update for the entire screen, and the session begins. Because of the stateless nature

of the client, either side can close the connection at any time without adverse consequences. The server can therefore choose the encoding most appropriate for the particular screen content being transmitted and the available network bandwidth.

C. VNC Viewers

In day-to-day use, we prefer the more descriptive term viewer to the rather overloaded word client. Writing a VNC viewer is a simple task, as indeed it should be for any thin client system. It requires only a reliable transport (usually TCP/IP), and a way of displaying pixels (either writing directly to the frame buffer or going through a windowing system).We have written viewers for all the networked display devices available at ORL. These include the Video tile (the original VNC viewer), an X-based viewer (which runs on Solaris, Linux, and Digital Unix workstations), a Win32viewer that runs on Windows NT and 95, and a Java applet that runs on any Java-capable browser (including Sun Java Station). Members of our abuse these viewers on a daily basis to access their personal computing environments [4].

D. Running a Viewer

When you run the viewer, you need to specify the name of the server and the number of the desktop. If, for example, you have started a server as display 2 on a machine called snoopy. you can start a viewer for it by typing: vnc viewer snoopy:2 With the Windows viewer, you can run it from the command line, but you will more typically run it from the VNC group on the Start Menu. In this case, you will be prompted for the host name and display number: Enter it and click OK, and you will be prompted for your password, after which you should see the remote display. If you are connecting to a Windows or Mac server, the display number will be 0, unless you have explicitly changed it. If the machine running the server does not have a proper DNS entry, you probably won't be able to use the name and will have to replace snoopy:2 with something like 192.168.1.2:2. You can get round this on most platforms by creating a host file which maps names onto IP addresses [4].

E. VNC Servers

Writing a VNC server is slightly harder than writing a viewer. Because the protocol is de- signed to make the client as simple as possible, it is usually up to the server to perform any necessary translations (for example, the server must provide pixel data in the format the client wants). We have written servers for our two main platforms, X (that is, Unix) and Windows NT/95.The X-based server was the first one we developed. A single Unix ma- chine can run a number of VNC servers for different users, each representing a distinct VNC desktop. Such servers can run on very simple hardware, and can be accessed from any of the standard VNC viewers.

F. Running a VNC Server

Install the Windows server, Win VNC, by running the Setup program included in the distribution. This will create a VNC group in your Start Menu. Install the default registry settings using the option in the VNC group. Run the WinVNC server. If this is the first time you used WinVNC on this machine you be prompted to set a password, which you need. when you connect to the machine from a remote location. Normally you want to leave the other options on their default settings (Note that the default display number is 0 on a PC. You need to specify this to the viewer when you connect). This avoids all the usual problems with fonts that plague X-emulators. In addition, because the session runs entirely on the server, if the viewer is stopped, the session remains and can be restarted exactly as it was when the viewer was stopped, which may even be on a different machine. The server and client then exchange messages to negotiate desktop size, pixel format, and encoding schemes. The client requests an update for the entire screen, and the session begins. Because of the stateless nature of the client, either side can close the connection at any time without adverse consequences.

G. Working of VNC

VNC can be executed from the command line with the windows viewer, but more customarily run it from the VNC group displayed at the Start Menu. In this situation, the host name has to be stimulated and number should be displayed: Enter it and click OK. Password will be required to proceed further, after which the remote display can be beamed. When a Windows or Mac server is associated then the displayed number will be 0, unless and until it is changed. If the machine operating the server lacks a proper DNS entry then no one will be able to access the name and have to compensate it. This can be administered on most platforms by contriving file which maps names onto IP addresses. Users may establish communication through Virtual Private Network (VPN) technologies, including instant VPN applications (such as LogMeIn Hamachi) to ease usage over the Internet, or as a LAN connection if VPN is used as a proxy, or through a VNC repeater (useful in presence of a NAT).

From Unix, Tight VNC will connect to a Mac OS X session served by Apple Remote Desktop if the VNC option is enabled, or to a VNC server running on Microsoft Windows. In July 2014 Real VNC published a Wayland developer preview [2].

IV. ADVANTAGES & DISADVANTAGES

A. Advance Features

The VNC protocol is very efficient at rendering areas of a single color, such as you generally find on window title bars, scrollbars, backgrounds of pages etc. A colorful or patterned desktop background will probably slow down VNC more than any other single factor. We have some suggestions on speed in t up the TWM window manager some of which will also apply to other environments. Hi-colour desktops. Don't use 24-bit colour if you can use 16 or 8 equally well. Remember, on Unix you can run multiple servers, so I have a big 16-bit desktop for normal work and a small 8-bit one for when I log in from home. The server can send out a wide range of pixel formats, and some viewers will allow you to request a specific format for that session. In advance the system will be developed as soon as the generation is established. Similarly, if you regularly connect to a remote Win VNC server, consider whether you could run happily at lower resolution. [3]

B. Advantages

1) It is usually used for controlling a proper functional system over a network from a disparate computer.
2) The VNC protocol is very utilitarian and robust as a cross platform explication.
3) Interchangeability is a clear advantage.
4) Unrecompensed, that is, it is free of cost and can be downloaded freely and used.
5) One of the prevalent benefits of VNC is that it is sharable which means that a single desktop can be exposed and used by various beholders at once, allowing Computer Supported Cooperative Work (CSCW) applications.
6) It is stateless, that is, the data can be apprehended efficiently from one system to another devoid of any interrupt.
7) Data can be accessed conveniently and efficiently without any need for installation.

C. Disadvantages

1) VNC is network resource intensive.
2) In case of low band width connection, an abominable situation emanates which means that a good bandwidth is required for its decorous functioning.
3) It is devoid of any modem access or features which is a detriment.
4) Display can be a bit sluggish, convulsive and incomplete.
5) File systems are apportioned between distinctive operating systems.
6) Exceptional multi-user support is not bestowed for accessing non-Unix platforms.
7) Various other mechanisms are obligatory for transferring files.
8) There is dearth of prevalent concept of several user accesses in PC/MAK.
9) Connection to VNC server can be contrived only through a direct IP address which makes both local and remote access arduous to set up.

V. Application

1) Bring up the controls for their video recorder on a mobile phone as they drive home from work.
2) Use a modem to dial a telephone answering machine and reprogram it through a graphical interface.
3) Display their car stereo or GPS receiver as part of the dashboard, regardless of the equipment brand installed.

VI. Conclusion

Virtual Network Computing (VNC), the area of virtual networks and remote terminal access has been explored. VNC is reasonably fast, it allows users to access remote terminals and that to very good speed. It allows user to simultaneously use two terminals. User can use VNC as a general purpose remote control product which allows handling of multiple terminals from a single terminal. It is very useful in all places where people working at different terminals need to access others terminals for various purposes.

References

[1] http://www.realvnc.com /RealVNC
[2] http://www.tightvnc.com /TightVNC
[3] http://fedoranews.org/tchung/vnc/index.shtml - FedoraNews.org
[4] https://hanyaketikanku.blogspot.com/2016/08/installasi-dan-konfigurasi-vnc.html

