Journal of Life & Physical Sciences

Available online @ www.actasatech.com

acta SATECH **2**(1): 37-39 (2005)

Research

Es-Spy: A remote network monitoring system

*Omotosho, O. J., Odim, M. O., Awodele, O., Akinlade, O. & Olubi, E.
Babcock University, Ilishan-Remo, Department of Computer Science & Mathematics, PMB 21244, Ikeja, Lagos 100 001, Nigeria

Received: 24 May, 2005 Revision accepted: 28 Oct., 2005

*Correspondence author <ojomotosho@hotmail.com>

Abstract

Managing multiple computers could be a colossal task. It could be almost impossible when the systems concerned are at a great distance from each other. Most network administrators find their job arduous because of the very little control they have over connected workstations. They find it difficult to contain defaulting users, or even know if users are defaulting in the first place. That raises the need for a remote administration tool, one that enables administrators monitor connected computers with little or no restrictions depending on the network configuration. This paper presents a remote administration tool, es-spy developed with Microsoft® Visual basic 6.0. and tested on windows XP Operating system with TCP/IP Protocols. It allows the administrator connect to workstations remotely. It gives the administrator "administrative rights" on the workstations, allows him change the remote computer's settings and more advanced option such as log off, restart, or even shut down. The paper suggests that the administrator should be in total control of the workstations regardless of physical limitations.

Keywords: Es-Spy, remote administrator, network computers, intrusion detection, key-logging

Introduction

Before now, the term "Remote Administration" didn't exist in the mainstream vocabulary. Gone are the days when networks encompassed a single building or campus. Now, networks could span geographic locations and involve the use of multiple protocols. The task of the network administrator is increasingly getting difficult. He/She cannot always be physically present at all locations. Sometimes, just one administrator has to attend to several users at the same time. At other times, the administrator is faced with a challenge of monitoring specific users, how does he/she accomplish these tasks without a remote administration tool?

Most networking management techniques are intrusion prevention based. However, Intrusion detection systems cannot by themselves completely protect a system from all forms of security threats (Graham, 2000). Many strategies, such as pass-wording, encryption, biometrics, to name a few, are employed to prevent access to unauthorized users to the network (Forcht, 1994). Nevertheless, the problems of network security still exist even if a user is authorized. For instance an authorized user, after gaining access can use the system for some task which he/she is not permitted to, such as children navigating unauthorised sites and the use of the system for some crime related activities. Hence the need for a system that can remotely monitor the activities of the users of the system in such a way that the administrator, through his/her computers can control these activities.

The needs for remote administration can be highlighted considering the following issues:

Cybercrime: One of the reasons why remote administration tools have become a necessity is the increasing number of computer-related crime. So much information is lost to hackers daily. An administrator should know what all connected users are doing, real time, and if he detects any misuse, he should be able to interrupt the user without his permission.

Technical Support: The administrator should be able to offer technical support to any connected user, without necessarily being present at the location. He should also have access to the system specifications remotely because technical support may depend on system specifications.

Remote File Access: The administrator should keep a tab on all files stored on remote systems. He could delete unnecessary or redundant files, upload updated copies of system files, or even download suspicious files from the remote system for scrutiny.

Dimarzio (2001) identifies the two main types of administrations:

Grounded Administration: This is a type of administration where the administrator is based in one location. The administrator has an office of his own where he monitors and controls the network.

Roaming Administration: For this type of administration, the administrator may manage different networks while moving from place to place. He may decide to manage the network from his home, on the road or any other place.

There is a whole world of difference between remote connectivity and remote administration as connectivity does not necessarily imply administration. There are two major ways of implementing remote connectivity (Dimarzio, 2001):

Dial-in Connectivity: Here, dial-in hosts such as Microsoft Remote Access Server. These servers accept connections and authenticate users. It is relatively inexpensive and the only hardware requirement is a modem.

Virtual Private Networks (VPN): This is a more secure remote connectivity tool. It offers the network administrator so much control over who joins the network.

Connectivity gives the administrator access to a system but administration gives him control over the system. As a network administrator, you need more than just ordinary access to the remote system, you need administrative privileges, and you need to be in control. Connectivity is not good enough to accomplish these tasks, they can only be achieved by the “Power of Remote Administration”.

The study aims at reducing the problems involved in the network administration such as limited access to the computer being administered. It provides a potential assistance to network administrator, helping him to know exactly what the user is doing. It will help to increase the efficiency and effectiveness of the administrator.

Material and methods

Programming

We employed an evolutionary development approach (Somemerville, 2004) to the development of *Es-Spy*, using Visual Basic 6.0. The program consists of two modules, the client and the server. The client runs on all remote systems while the server runs on the administrators system. When the administrator makes a command (such as restart), a code is sent to the appropriate client and the task is executed on the client using the Application Programming Interface (API). There are a total of One Hundred and Four (104) total commands that can be executed on the clients by the administrator.

System Features

The features of the system are outlined below:

Intrusion Detection: Es-spy allows administrator to detect any intruder on the network. This is possible because every client broadcasts a certain line of code to the server which enables it detect new connections.

Key Logging: Es-Spy has a key–logging feature that enables the administrator log everything a user is typing on his key board. This is an advanced security feature. It is a way of remotely watching what is been typed on a remote computer

Clipboard Data: Whatever data is on the clipboard of a remote system can be viewed by Es-spy. In other words, the administrator can view what a user copies and can paste it on his own system, further than that, the administrator can also set a clipboard text on a remote system and the user can paste it.

Information Acquisition: Administrator can request for information about a remote system. Information that can be requested include, Operating System product ID, O\S Product Key, Operating System, Program files Directory, O/S version.

Manual Control: Es-Spy gives the administrator control over manual processes such as opening and closing the CD-ROM drive of the systems.

Es-Spy System Requirement

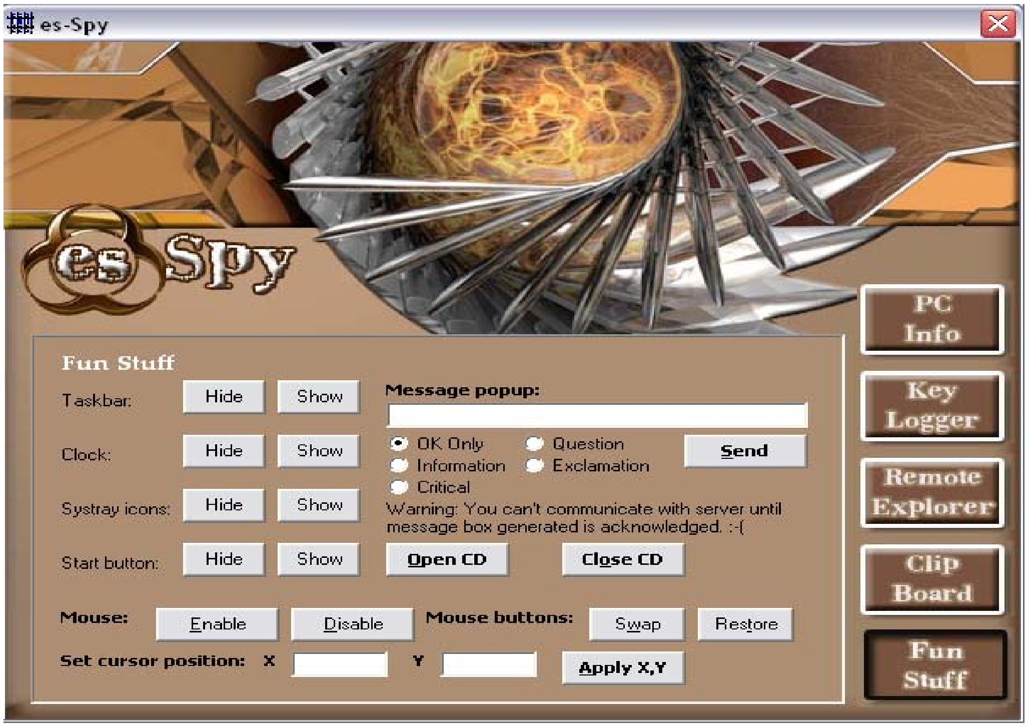
Micrsoft windows 98; 64Mb of RAM; 1 GB of Hard disk; Pentium 1 with network card and connection.

Test-bed platform

The Es-Spy was tested on a local network (Client server system) with Windows XP using IP/TCP.

Results and Discussion

Es-Spy is a remote monitoring tool we developed to solve the identified problems (Fig. 1). It can be used to administer any computer system across a network. Administration includes remotely watching what is being typed on the system, viewing clipboard data, checking remote system’s configuration, remotely browsing the file system which allows you to download files from the remote system, upload files to any folder you want on the remote system or even create your own, change remote system’s wallpaper. Other possibilities include the ability to get and set remote system’s cursor position, swap mouse buttons,



● OK Only

Warning: You can't communicate with server until message box generated is acknowledged. :-(

Fig. 1: The es-Spy interface

or even disabling the mouse. You could also log off, restart, or even shut down the remote system. Advanced features (such as log off, restart, or even shut down) allow you to create and edit registry entries provided the user logged on to the remote system has administrator rights.

The software is actually divided into two parts, the client- and the server-side. The client application is the one used to access the remote system, and the only one with a graphical user interface. The server application runs invisibly on the remote system. It accepts connections from the client application and subsequently executes commands sent from the client application. The server application must be running on the remote system before the client application can be used to connect to it. This means that the server application can only be started by someone who has physical access to the remote system. This prevents illegal monitoring of remote systems and possible intrusion of remote user's privacy. This makes es-Spy a tool of choice for parents wanting to monitor their kids' activities.

Es-Spy can be used across any network. It can be used across the Internet as long as both systems are directly connected to it or connected through an ISP, but not when any of the systems is part of an organizational network, this is because of firewalls and proxies used in various organizations with an Internet connection.

The Administrator's interface (Fig. 1) consists of the following main menus:

PC info: allows the administrator to request for system information on the client system.

Key logger: lets the Administrator access to files on remote system.

Clip board: requests clipboard data.

Fun stuff: allows administrator to enable or disable remote system's task bar, start button clock, mouse, system tray icons, etc.

Conclusion

It is very obvious that remote monitoring (administration) is the future of Network management. Networks will be managed remotely by parents, teachers etc. to monitor their children and students for good causes. Hence, we can all harness the power of remote administration and make it work for a good cause.

Reference

Dimarzio, D. F. 2001. Network Architecture & Design. SAMS Publishing.

Eric, A. F. & Gregory, B. W. 2000. *Secure Computers & & Networks*. Florida, CRC Pres Inc.

Graham, R. 2000. FAQ Netwowrk Intrusion Detection Systems. http//secinf.net/intrusion_detection/FAQ_network_intrusion_detection_system_html

Poch, U. W., Machuel, D. & Mccalin, J. 1991. *Telecommunications and Networking*. Florida,CRC Press Inc

Somemerville, I. 2004. Software Engineering, 7th ed. England, Pearson Education Ltd.