International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP418-423

A Remotely Access and Anti-Theft System (R2AS)

Manoj Awate[1], MayurChabukswar[2] , Mahesh Mokate[3] , Sanjay Lohar[4]

[1234]*(Comp. Department, University of Pune, India.)*

Abstract :- this project deals with a collection of security-related functionalities of the terminal systems connected through a network. This system implements Remote control and security at the application level.We have already universal remote control devices for controlling consumer electronic devices. Similarly, we may control our desktop and laptop PCs and their applications remotely via portable and smaller computers like PDAs and Pocket PCs. This paper presents a system and its architecture that enables a wireless enabled PDA to control a PC and its applications remotely over an internet.

Keywords :-AE, encryption data, R2AS,Remote access,self-destructing data.

I. INTRODUCTION

Controlling consumer electronics devices and computers remotely is an important as aspect of the technology. Today, we have universal remote control devices to control consumer electronic devices such as TV sets. Similarly, it is desirable to remotely control stationary desktop/laptop PCs and their applications. For example, an instructor in class-room may want to control a PowerPoint presentation running on his laptop computer and projected on the screen using a PDA (i.e. pocket PC) or cell phone, while he is moving around in the class-room freely. In this way, he does not have to go to the laptop each time when he wants to update the PowerPoint screen. This paper is about how to control PC applications remotely inside a house, an office, or a conference room. As the remote control device, we consider using a general purpose pocket PC computer with wireless LAN or PAN capability (i.e. supporting Wi-Fi).

It consists of two parts: a server part and a client part. The server part runs on a desktop PC (or laptop PC depending on the usage scenario) to be controlled remotely. The client part runs on a mobile Pocket PC device that can be easily carried by a user and that will act as the remote controller device for desktop PC and its applications. The server side of the system is capable of listening incoming connections, sending and receiving data, processing control commands, taking screenshots, modifying and sending images back to client side, and sending mouse and keyboard events to the operating system.

Remote desktop access is the most convenient way to telecommute and remote maintenance, but it also brings insecurity problems in supervision and auditing. Because of no transparency among RDP, VNC, X-window, it often brings in security problems of resource abusage and breach of confidence, which are difficult to ensure security supervision and content inspection from external security tools. It is necessary to adopt effective mechanism to monitor and audit towards remote graphics operations, especially for those crucial servers with key data. In this paper, a novel proxy-based security audit system is designed and implemented in order to ensure security supervising and auditing for remote desktop access. Our system monitors all the accessing sessions of RDP, VNC, and X-window by using proxy technology, And provides replay function by recording all the graphics operations from end users. And our performance test results show that for most of small business, only one proxy server is enough to handle the routine auditing workload of RDP sessions. The remainder of the paper is organized as follows.

We identified the following as the requirements of a system that enables a Pocket PC to be used as a remote and mobile control device for desktop PC applications. Those identified requirements helped us as the basic guidelines in designing our system.

• *Ease of use*: The system should be easily launched, Configured and used. It should have a nice and graphical User interface.

• *Mobility*: The system should support mobility of the User while controlling the desktop computer application. Mobility can be enabled if the remote control device is Portable and if its connection to the desktop computer is wireless. The wireless connection can be a short-range local or personal area connection, most of the time. In that case, the roaming range can be up to 100 or 300 meters depending on the wireless technology used and on the propagation environment.

• *Flexible Control*: A user should be able to control and execute as much functionality as possible. It is the best if the user can do everything that he/she can do on a desktop computer also in a remote manner. The user should be able to give keyboard inputs and mouse inputs to the desktop PC and also should be able to get as much screen information as possible.

• *Power*: The system should be power efficient since the PDAs are power constrained devices and have limited energy.

• *Reliability*: The system and connectivity should be reliable enough so that a user can control the desktop computer without losing data and/or commands.

• *Bandwidth*: The system should be bandwidth efficient on the wireless link between the PDA and desktop PC, since the same link can be used for many other applications that are run at the same time, like an FTP transfer, a web browser activity, a backup activity, and so on.

• *Enabling Feedback*: While interacting with the desktop PC using a mobile PDA, the user should get enough feedback from the system about what is going on and about the status of the executed operations.

• *Asymmetric Functionality*: A desktop computer has advantages in comparison to a Pocket PC in terms of computation power and unconstrained energy sources. Therefore the system design should be asymmetric whenever possible, giving more computational overhead to the server side of the system than the client side. In other words, a thin client model is a preferred model for the architecture of the system.

1.1.Applications of R2AS

Remote Access can be used for wide range of Applications such as, in defenceorganisations for safe circulation of secret data. Colleges can use it for securing faculties, exam papers , student information etc. In companies it can be used to provide secure highly confidential data.

1.2.Features of R2AS Techniques

1.2.1.Controlling system throws cell phone i.e. by sending Shutdown, restart and sleep command.

SHUTDOWN/RESTART/SLEEP-we can controlour pc from Remote place so we can even shutdown our Pc with our Android device. We just have to Click one button and other work will done by System automatically. Fig 1.1 shows the working

Fig 1.1 User Send a command to shutdown a remote device

1.2.2. Sending snapshot of unauthorized user on cell phone
When any unauthorized user wants to access the PC (R2AS secure) than software will automatically detect the user as a unauthorized user and send the snapshots of that user to the user of system.

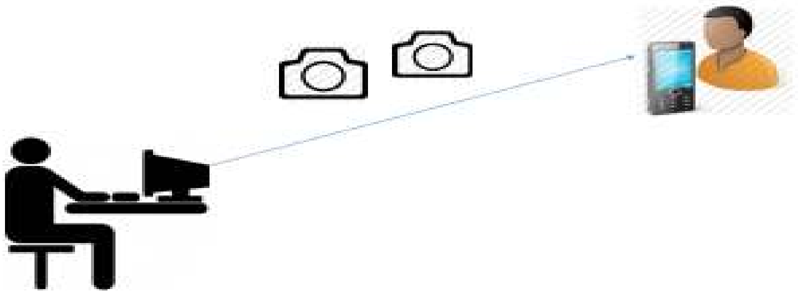

Fig 1.2.Snapshots send to authorized person of the system.

1.2.3. Controlling Unauthorized Access

If password entered for accessing important folders 3 times is invalid then send backup of data in encrypted form to Google drive before executing self-destroying program

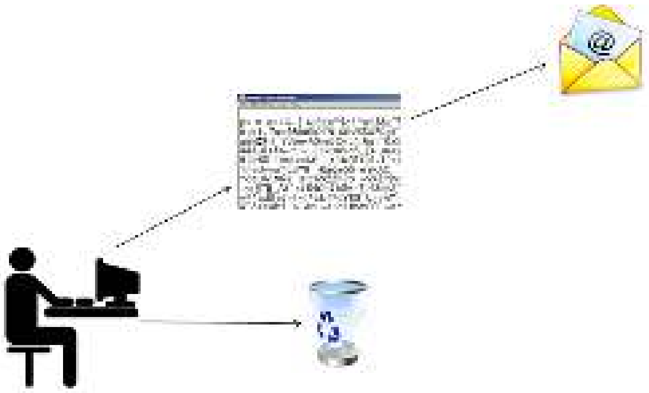

Fig 1.3 If unauthorized access encrypt and send data to mail.

II. ARCHITECTURE

Client server Architecture in which client send the request and wait for server to respond. After receiving response. Client can resume its processing. In this type of architecture many clients (remote processors) request and receive service from a centralized server (host computer).

2.1. SOFTWARE ARCHITECRURE:

Client computers provide an interface to allow a computer user to request services to the server and to display the results, the server returns. Servers wait for requests to arrive from clients and then respond to them. Today clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful machines. This computing model is especially effective when clients and the server each have distinct tasks that they routinely perform.

Whenever user wants to access the system, he runs the application on his android phone and broadcast the request to establish the connection on the network using IP address and the server whose IP address matches the broadcasted IP address will accept the request. Then server sends an OTP message for authentication to the client and when it is validated then the connection is established.

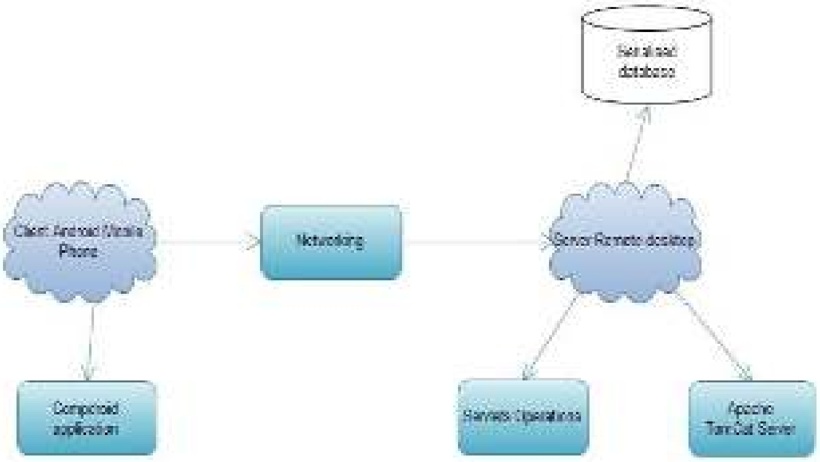

Fig.3 System Architecture

III. PROPOSED SYSTEM

In earlier projects VNC architecture is used which is basically implemented on Linux Operating system, but we are building a more generalized system which is based on Client server architecture. Previous projects can't turn on the remote desktop explicitly but we are providing the same using GSM modem.
The modules used in our project are as follows:

3.1. Module 1: Login

It is the first module which the user will face. The login module contains the User ID and Password which on verification by server will provide the authentication to user. If you need to secure an application you have developed, you can do this using your own login module. This login module allows you to perform authentication. We are using Java for creating our modules with the J2EE Engine. The login modules must compare a client-supplied password to a password stored in a user management system. These modules generally work with plain text passwords, but can be configured to support hashed passwords to prevent plain text passwords from being stored on the server side.

3.2. Module 2: Capturing Image

A screen dump, screen capture, screenshot, screen grab, or print screen is an image taken by the computer user to record the visible items displayed on the monitor, television, or another visual output device. Usually, this is a digital image using the operating system or software running on the computer, but it can also be a capture made by a camera or a device intercepting the video output of the display. That latent image converted and saved to an image file such as to JPEG or PNG format is also called a screenshot.

This module will take a screenshot of the remote desktop and then using the scaling algorithm it is resized according to the mobile resolution and sent to the client mobile. This information is updated as the screen changes or according to the timer. If the timer is set to 2sec then the server will send a new screenshot after every 2sec to the client android mobile.

3.3. Module 3: Forward Keyboard Shortcuts

This module uses the reference of the keyboard shortcuts.Typing “Ctrl+c” is very difficult or we can simply say it's impossible, hence we are providing the same to the user for its better convenience. This module will store the ascii code of the “ctrl” and “c” in the proposed shortcut and whenever the user will press the shortcut then the server will forward the code to the user desktop machine. The basic keyboard shortcuts we are providing to the user in this module are:

Table 1

Name of Shortcut	**Shortcut**
New window	“Ctrl+n”
Copy the selected text	“Ctrl+c”
Paste the copied text	“Ctrl+v”
Cut the selected text	“Ctrl+x”

3.4. Module 4: Mouse Operations

The mouse operations are very basic operations for the user and provide a great comfort to the non-professional user while interacting with computer, hence this module is included in our project.As the right-click and double-click is very difficult on mobile phone, so we are providing the shortcuts of the same. We are just storing the key value on the server machine and whenever user will press the shortcut then the key value is passed to the application.

The basic mouse operations shortcuts we are providing to the user in this module are:

TABLE 2

Name of Shortcut	**Shortcut**
Left click	Mouse Left click
Right click	Mouse Right click
Double click	Mouse Double click

3.5. Module 5: Text on Fly

The meaning of text on fly is literally the text is flying. Here the text is flying from the client machine to the server machine. The basic idea is user will type the text on the client mobile in a textbox and whenever the user is conformed with its text then that text is sent to the remote desktop.

3.6. Module 6: Application Shortcut

Application shortcut are created for accessing various application like for accessing notepad, MS-Word, Games, etc...

These help by saving time and reducing the complexity as the applications which are most often used are stored as shortcuts so that to operate the application only shortcut will do (no need to follow same lengthy path all the time).

IV. Future scope

In future Home appliances can be controlled using Comp droid. We can use this system in colleges for sharing the remote desktop by student during practicals.

V. Conclusion

In conclusion, Remote Desktop and Remote Desktop Web Client are becoming more and more popular to meet the remote control needs of corporate IT and the telecommuter. Microsoft has taken good steps to ensure security of this Technology documented above by its much strength and few weaknesses. Nothing is ever 100% secure, but having an understanding of the technology, using what tools are available for auditing, and following a defense checklist will help you make your environment as secure as it can be.

REFERENCES

[1] ArchanaJadhav, "VNC ARCHITECTURE BASED REMOTE DESKTOP ACCESS THROUGH ANDROID MOBILE PHONES", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 2.

[2] Vipul Daladier , Stuart Marshall , Ian Welch "USING REMOTELY EXECUTING SOFTWARE VIA A MOBILE DEVICE"

[3] BuntarouShizuki, "VNC-BASED ACCESS TO REMOTE COMPUTERS FROM CELLULAR PHONES"
Timothy Vidas ,"ALL YOUR DROID ARE BELONG TO US: A SURVEY OF CURRENT ANDROID ATTACKS"

[4] ChaitaliNavasare, DeepaNagdev and Jai Shree, "POCKETDROID - A PC REMOTE CONTROL", 2012 International Conference on Information and Network Technology (ICINT 2012) IPCSIT vol. 37 (2012)

[5] R.Manikandasamy , "REMOTE DESKTOP CONNECTION USING MOBILE PHONE", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 8, August 2013

[6] AjitKotkar and AlokNalawade, "ANDROID BASED REMOTE DESKTOP CLIENT", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2013

[7] SonamGavhane , "REMOTE DESKTOP ON MOBILE" , International Journal of Innovations in Engineering and Technology

[8] (IJIET)

[9] K.S. Kuppusamy, "A MODEL FOR REMOTE ACCESS AND PROTECTION OF SMARTPHONES USING SHORT MESSAGE SERVICE", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012

[10] .Dhananjay .A.Sherigar ,"3 FACTOR AUTHENTICATION FOR REMOTE ACCESSING USING ANDROID DEVICE ", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 2, February- 2013 ISSN: 2278-0181