IP Camera and Mobile based Remote Login Intrusion Detection

Bharathi M A [1], Mallikarjun Mathad [2], Gururaj S P [3]
[1]bmalakreddy@yahoo.com
[3]gururajsp@yahoo.co.in
[1]Department of Computer Science and Engineering
[2]Department of Information Science and Engineering
Reva Institute of Technology and Mangement

Abstract- *Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques*

When a user of an information system takes an action that user was not legally allowed to take, it is called *intrusion. Internal intruders* have legitimate access through user accounts; *external intruders* break into a system without benefit of a user account A server is a system which keeps running continuously and the administrator cannot monitor the system all the time .Any unauthorized user should not be able to use the server system and any event done by him should be known to the administrator. The events can be anything from simple mouse to keyboard interruptions (events). As information systems have come to be more comprehensive and a higher value asset of organizations, complex, *intrusion detection* subsystems have been incorporated as elements of operating systems, although not typically applications. Providing security for the admin system where he can control and monitor the server by getting alert messages both text and image or photo by using IP camera, when unauthorized person tries to access the system .He can shutdown the system or kill the process by sending the message to server.

Key Words: *AT Command, anomaly detection, GSM MODEM,SMS gateway*

I. INTRODUCTION

When a user of an information system takes an action that user was not legally allowed to take, it is called *intrusion*. The intruder may come from outside, or the intruder may be an insider, who exceeds his limited authority to take action. Whether or not the action is detrimental, it is of concern because it *might* be detrimental to the health of the system, or to the service provided by the system.

As information systems have come to be more comprehensive and a higher value asset of organizations, complex, *intrusion detection* subsystems have been incorporated as elements of operating systems, although not typically applications. Most intrusion detection systems attempt to detect suspected intrusion, and then they alert a system administrator. The technology for automated reaction to intrusion is just beginning to be fashioned. Original intrusion detection systems assumed a single, stand-alone processor system, and detection consisted of post-facto processing of audit records. Currently there are two basic approaches to intrusion detection. The first approach, called **anomaly detection**, is to define and characterize correct static form and/or acceptable dynamic behavior of the system, and then to detect wrongful changes or wrongful behavior. It relies on being able to define desired form or behavior of the system and then to distinguish between that and undesired or anomalous behavior. The boundary between acceptable and anomalous form of stored code and data is precisely definable. One bit of difference indicates a problem. The boundary between acceptable and anomalous behavior is much more difficult to define. The second approach, called **misuse detection**, involves characterizing known ways to penetrate a system. Each one is usually described as a pattern. The misuse detection system monitors for explicit patterns. The pattern may be a static bit string, for example a specific virus bit string insertion, and alternatively, the pattern may describe a suspect set or sequence of actions.

We are now in the third generation of operating system based intrusion detection where networks are a major focus and their concern is to manage the volume of data, communications, and processing in large scale networks, increase coverage (i.e. be able to recognize as much errant behavior as possible), decrease false alarms (benign behavior reported as intrusion), detect intrusions *in progress*, and react in real-time to avert an intrusion or to limit potential damage. The remaining parts are organized as follows. Section **I1** describes the related work done in intrusion detection.. Under the basis, intrusion d**etection approaches** in existing system **done in sec**tion**111.** Section **IV** talks about the proposed work. Further implementation discussions on the basis are conducted in section V. Finally, we draw results, tests and conclusions and lay out future works in section VI.

II LITERATURE SURVEY

Amir Vahid Dastjerdi, Kamalrulnizam in their work tries to offer a line of defense by applying Mobile Agents technology to provide intrusion detection for Cloud applications regardless of their locations.[1]. Another work described in [2] uses a four components Manager, Assist MA, Response MA and Host monitoring agent. Each monitored in the network installed with host monitoring agent to implement intrusion detection. Authenticating the user to the mobile device provides security against unauthorized use, but it includes difficult security issues: the method may be weak, authentication information is often seldom changed and the management of authentication information is difficult in enterprise use [3]. In this paper we propose a distributed intrusion detection system for ad hoc wireless networks based on mobile agent technology. Wireless networks are particularly vulnerable to intrusion, as they operate in open medium, and use cooperative strategies for network communications.[5]

III EXISTING SYSTEM

Authorized user will be given user name and password. Using that username admin can lock the system but there is a problem in this type of locking. An intruder may delete the account or change the password. Windows (Desktop) Lock is computer security protection and access control software can be used to lock computer to prevent people from accessing your private documents and resources. Passwords are inherently weaker than a large binary key value. Windows locks can be easily hacked One possible method is to reboot in safe mode and access safe mode admin account and remove actual user's password, Administrator will never know about the intrusion.

IV PROPOSED SYSTEM

The proposed Intrusion Detection System detects hostile activities in a network and possibly prevents activities that may compromise system security and an ability to provide a view of unusual activity and issue alerts notifying administrator and/or block suspected connections.

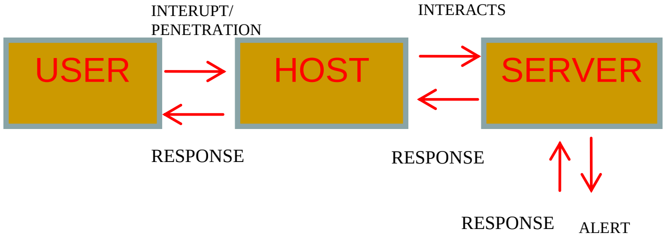


Fig. 1 Block Diagram of the Proposed System

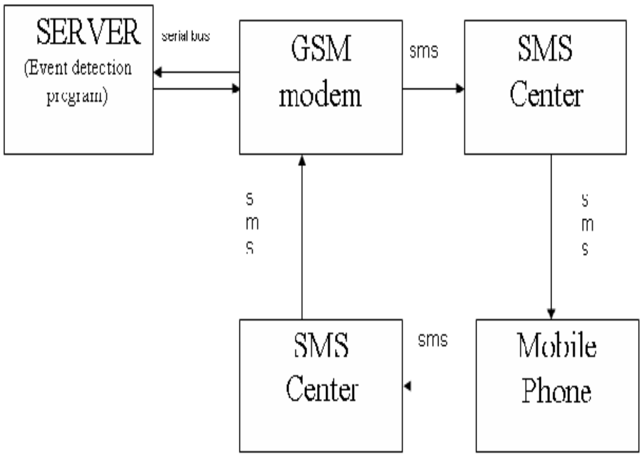


Fig 2. Architectural Design of the Proposed System

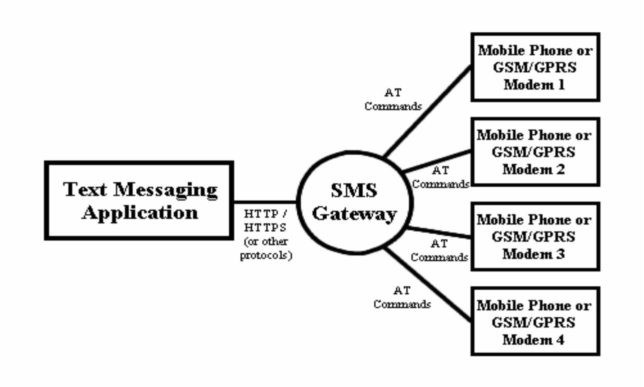


Fig 3.An SMS text messaging application connects to a pool of mobile phones or GSM/GPRS modems through an SMS gateway.

Intrusion when sensed sends alerts to admin using Mobile device we can control the system by sending commands like shutdown, kill a process, block keyboard etc. The main components that form the system design of our proposed system are: Server or a PC, GSM MODEM and Administrator's Mobile phone. The server contains lot of important data and will be providing services to lot of clients. The GSM MODEM is connected to the server through a serial port, The event detection program will be running in the server which monitors for any mouse and keyboard events. If there is any occurrence of either mouse or keyboard event while the administrator is away from the server the event detection Program will detect the intrusion and it communicates with the GSM MODEM using AT commands. AT commands are the commands which are used to communicate with MODEMs. In this case we communicate with the MODEM to send an SMS alert to the Adman's mobile device through the SMS center of the network provider of GSM MODEM. The program running in the server will also disable the mouse and keyboard thus blocking all inputs from the mouse and keyboard. As soon as the Admin receives the SMS alert he will respond back by sending an SMS back to the GSM MODEM through the SMS center of the network provider from the Adman's mobile phone. The message sent to the GSM MODEM is stored in its memory and the program running in the server will read the message from the memory of the GSM MODEM and if the sent message is any of the commands defined then appropriate action will be performed by the server, in this case if the message read is "shutdown" the server performs a shutdown operation or if the message contains "kill" then the server will enable the mouse and Keyboard unblocking the inputs from keyboard and mouse. To send SMS messages, first place a valid SIM card from a wireless carrier into a mobile phone or GSM/GPRS modem, which is then connected to a computer. The instructions used for controlling the mobile phone or GSM/GPRS modem are called AT commands. (AT commands are also used to control dial-up modems for wired telephone system.) Dial-up modems, mobile phones and GSM/GPRS modems support a common set of standard AT commands. In addition to this common set of standard AT commands, mobile phones and GSM/GPRS modems support an extended set of AT commands. One use of the extended AT commands is to control the sending and receiving of SMS messages.

An IP Camera is a stand-alone device which allows you to view live, full motion video from anywhere in the world. IP Cameras can be used for surveillance of both homes and businesses. With the ability to record live video to a remote location, IP Cameras allow you to make sure your recorded video is safe by storing it at a location that only you can access.

Fig 4 An IP Camera

The larger the facility being secured, the more valuable an immediate transition to IP cameras. The more mature mega pixel cameras become, the more valuable an immediate transition to IP cameras.
DVRs will continue to catch up to NVRs and will as such extend the life of analog systems.

V Implementation

AT commands are sent to a mobile phone or GSM/GPRS modem by using a terminal program. A terminal program's sends the characters you typed to the mobile phone or GSM/GPRS modem as shown in fig 5. It then displays the response it receives from the mobile phone or GSM/GPRS modem on the screen. A code to use AT commands and the HyperTerminal program of Microsoft Windows to send an SMS text message is shown in Fig 4. The lines in bold type are the command lines that should be entered in HyperTerminal. The other lines are responses returned from the GSM / GPRS modem or mobile phone.

```
AT
OK
AT+CMGF=1
OK
AT+CMGW="+85291234567"
> A simple demo of SMS text messaging.
+CMGW: 1
OK
AT+CMSS=1
+CMSS: 20
OK
```

Fig 4 Code Snippet for SMS text messaging

The following is the code snippet for disabling keyboard and mouse.

```
Public Class Form1
    Private Declare Function BlockInput Lib "user32" (ByVal fBlock As Long) As Long

  Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles MyBase.Load
    End Sub
Private Sub Form1_Shown(ByVal sender As Object, ByVal e As System.EventArgs) Handles Me.Shown
        Dim now As DateTime = DateTime.Now
        While ((DateTime.Now.Subtract(now).Seconds < 1000))
            BlockInput(True)
        End While
        BlockInput(False)
        Label1.Text.Insert(0, "InputEnabled")
    End Sub
End Class
```

Fig 5 Code snippet for enabling keyboard.

The only way to enable keyboard and mouse is by sending "kill" command to the GSM modem which is read by the program which will terminate the process which blocks the input by executing system command "task kill" with the process name as the argument.

VI Results

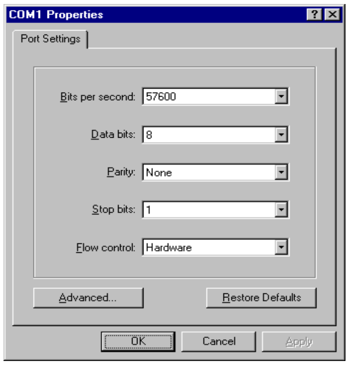
Testing the COM port number to communicate with the GSM modem and testing the route status in the GSM modem after the status information is received by the ADMIN .The Messages are displayed throughout the end of the application. The Acknowledgements will be received by the ADMIN after the events are occurred in administrator account. The messages are sent to ADMIN if and only if any unauthorized person tries to use the account as shown in Fig 6.The Status of GSM modem information is done automatically in the server.

Threats tested:

Name	***Breaking into the and peripherals server, computer***
Description	Attacker gains access to the devices /peripherals ,Server, computer's operating system and files.
STRIDE Classification	Spoofing identity Tampering data Information disclosure Denial of service Elevation of privilege Touch to peripherals
Mitigation	Protecting operating system's user accounts With passwords. Avoiding unnecessary Software. Reducing of open TCP ports. Patching and keeping all software up to date
Entry point	Peripheral held ,Server computer, locally or remotely Protected
Protected resources	All H/W of the system data at computer and server.

Table 1 Test of threats from intrusion detection done.

The IP Camera used in the implementation helps in viewing the intrusion and detecting it and remotely assisting others ,Supervising computer or internet usage and Access to a remote system's "Computer Management" snap-in



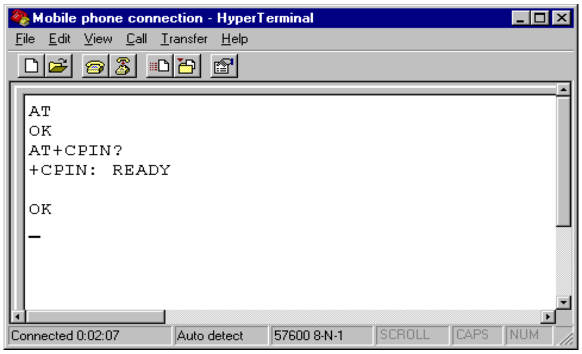
Bits per second: 57600

Data bits: 8

Parity: None

Stop bits: 1

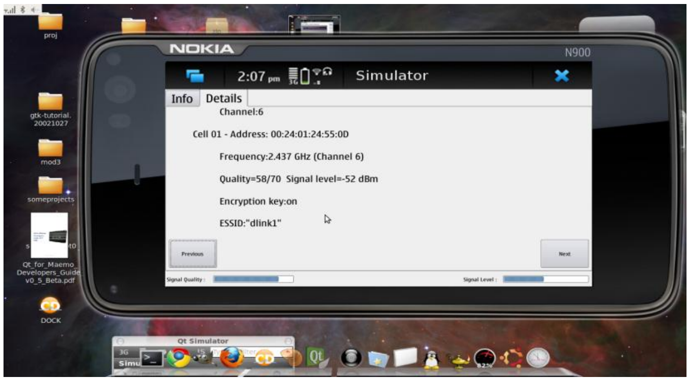
Flow control: Hardware


Mobile phone connection - HyperTerminal
File Edit View Call Transfer Help
Connected 0:02:07
Auto detect
57600 8-N-1
SCROLL
CAPS
NUM

```
AT
OK
AT+CPIN?
+CPIN: READY

OK
_
```

Fig 7 Screenshot of MS HyperTerminal's



Channel:6

Cell 01 - Address: 00:24:01:24:55:0D

Frequency:2.437 GHz (Channel 6)

Quality=58/70 Signal level=-52 dBm

Encryption key:on

ESSID:"dlink1"

Fig8. Alert SMS on Admins Mobile

VII Conclusion

In this proposed system we present the motivation of an approach that solves the basic security level which depicts the foundation of our architecture/ system and exposes results obtained from prototype and implementation. The proposed system keeps track of the main threat from internal intruders, those with limited authority seeking to extend the authority particularly in the context of their application. We hypothesize that application specific intrusion detection systems can use the semantics of the application to detect more subtle, stealth-like attacks such as those carried out by internal intruders who possess legitimate access to the system and its data and act within their bounds of normal behavior, but who are actually abusing the system.

References

[1] Amir Vahid Dastjerdi, Kamalrulnizam Abu Bakar, Sayed Gholam Hassan Tabatabaei, "Distributed Intrusion Detection in Clouds Using Mobile Agents," ***in advcomp, pp.175-180, 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009.***

[2] Shao-Chun Zhong, Qing-Feng Song, Xiao-Chun Cheng,and Yan Zhang, " A Safe Mobile Agent System for Distributed Intrusion Detection," in ***Proc. of the International Conference on Machine Learning and Cybernetics, Vol 4,pp 2009-2014, Nov 2003.***

[3] Gavrila, S., Jansen, W. & Korolev, V. "Proximity Beacons and Mobile Device Authentication: An Overview and Implementation", *NIST Interagency Reports 7200*. 2005.

[4] Z. Li. A. Das, and J. Zhou, "Unifying Signature-based and Anomaly-basedIntrusion Detection," in ***Proceedings of the Ninth Pacific-Asia Conference on Knowledge Discowry and Data Mining (PAKDD-O5),*** (Hanoi, Vietnam), Lecture Notes in Artificial Intelligence, May. *2005.*

[5] Oleg Kachirski ,Ratan Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", ***HICSS '03 Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 2 - Volume 2.***

.