Second level Security using Intrusion Detection and Avoidance System

Chayashree G
Asst. professor ISE Dept.
GSSSIETW, Mysore, India
chayashreeg@gsss.edu.in

ABSTRACT

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic. So in this proposed system it has enhanced the security for a common application running in PC's that are connected by a LAN. Here the system has provided a controlled access to that application through the login form. In case an intruder tries to access the application with incorrect password and username then server will get notified after a specific number of trail and a notification message will be send to the administrator mobile through GSM modem. The PC through which the intruder had tried to access the application will be automatically gets shutdown as he finishes his available trials. Hence the intruder will be avoided from accessing application once again after the specific number of trial. Once the Administrator knows the situation he may take action accordingly. So the application is protected from the unauthorized access. By doing this the proposed system provided an second level of security.

Index Terms—IDS, Malware, integrity (key words)

I. INTRODUCTION

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malwarer and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses. Generally intrusion detection system (IDS) monitors for suspicious activity and alerts the system or administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. An IDS installed on a network provides much the same purpose as a burglar alarm system installed in a house. Through various methods, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning or alert.

Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain intrusion detection systems have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event.

II. Background

IDS system is required here to detect attacks against computer network and notify us when the attacks occur. An Intrusion Detection System (IDS) is the high-tech equivalent of a burglar alarm. A burglar alarm configured to monitor access points, hostile activities, and known intruders. The simplest way to define IDS might be to describe it as a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers, and other network devices.

IDS can provide an after-the-attack audit trail for seeing how far an attacker got, and where it came from to eliminate the problem by having the Intrusions Notification via SMS. The transformation to the new will be system hopefully will give benefit for systems administrator. With the SMS alert system hopefully it can reduce time required by systems administrator to monitor intrusion/threat in the network and also give systems administrator enough time to do multitasking job function in networking environment.

2.1 Purpose of the situation

In this fast moving world people are handling lot of devices for their personal use that should be handled properly. Security is one of the main aspects of the modern world. People expect their personal devices and data to be secure from unauthorized access which otherwise leads to data and economical losses. The main aim is ensure security of a personal computer and alert the administrator through sms.

2.2 Target user

The target user in the proposed system is the clients. It is usually used in the LAN connection with the client and server. The administrator will know who the authorized and unauthorized users are. The mainly its target to the small organization which performs the simultaneous task performed by each individual employees in that organization.

2.3 Problem context and rationale

The system needed to be designed simple to use and easy. The system built will be unlocked only with the help of correct password. The server will be monitoring the all connected client systems to it. The authenticated users are able to use the systems while unauthenticated users are not allowed to use the system. The admin should able to get the text message upon a wrong password trial by an unintended (unauthenticated) user. After sending the message to the admin mobile the system will get shutdown.

2.4 Objectives of the system

The main objective of the system is to alert the server system when an intruder is found. The server gets notification from the client systems irrespective of the users. The alert notifications are stored in database where they can view later. The alert notification of an intruder can be identified by the administrator system through the inet address of the particular client system and that system is shut downed.

III. PROBLEM DESCRIPTION

3.1 Current problem description

The current trend in companies is allotting the jobs for the individual or providing the username and password for accessing the certain application. So that system user cans the access application installed by username and password authentication in current situation. And the user may use and get access to it. If the unauthenticated users try to access he will not be able access the application then he make as many as tries to access it. But the system administrator is unaware of the situation. Hence in order to know the intruder in the connections an application has to be built. An application build should be simple and easy to use.

3.2 Proposed solution

Here the proposed system enforces a second level of security by using an intrusion detection system above the primary login id and password. An intrusion detection system is used to detect several types of malicious behavior that can compromise the security and trust of a computer system. The proposed systems intend to avoid the access and keep track of the intruder's attempts and intentions. The usual way to enforce security to the client computer is through the use of the login id and admin password the inet address of the particular client system is known to the server. Upon number of trials from the unauthorized person server system sends the text message to the admin mobile and automatically the client system will get shutdown.

IV. DESIGN

4.1 System design architecture

System Design is a modeling process. It is a solution how to approach to create a new system. It can be defined as a transition from user's view to programmer's or database persons view. The design phase mainly depends on the detail specification in the feasibility study. The design phase acts as a bridge between the proposed system and the required specification and the implementation phase.

Server:

The below shown figure is the sever system architecture. It includes login for the server which is used to authenticate the server, server program will be running behind which used to know the client details and connected GSM modem kit to it used to send the message to the administrator mobile.

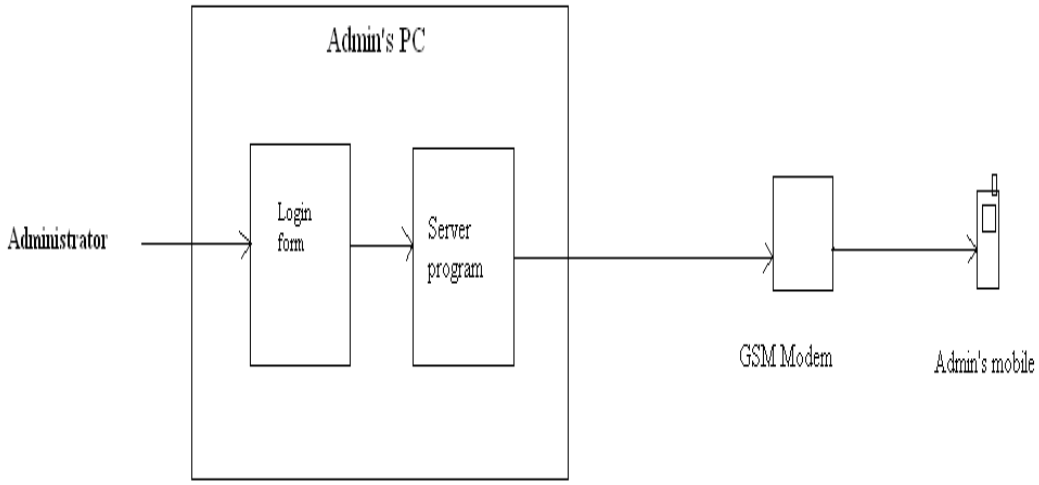

Fig 4.1 Server system architecture

Client:

The below shown figure is the client system architecture. The features available for the security of client application are as shown in the figure. It includes similar login page as in the server, in case of unauthenticated access the system automatically get shutdown.

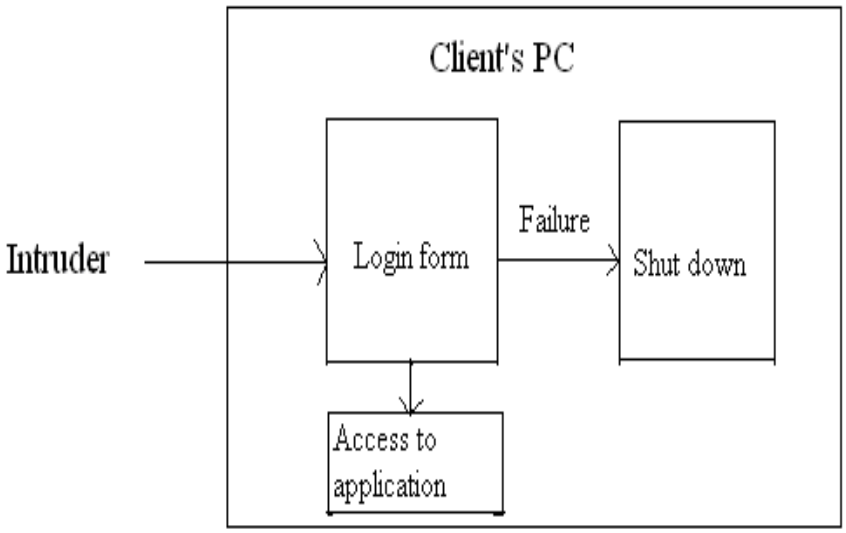

Fig 4.2 Client system architecture

4.2 System flow charts

- **for alerting Admin:**

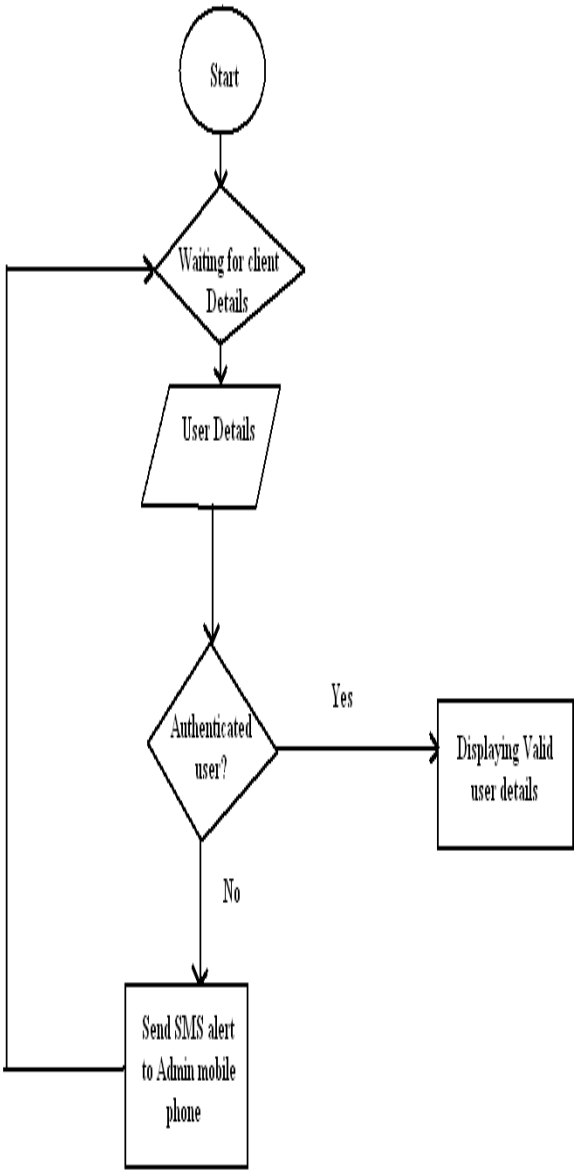

Fig 4.3 system flow chart for alerting admin

- **for server login module:**

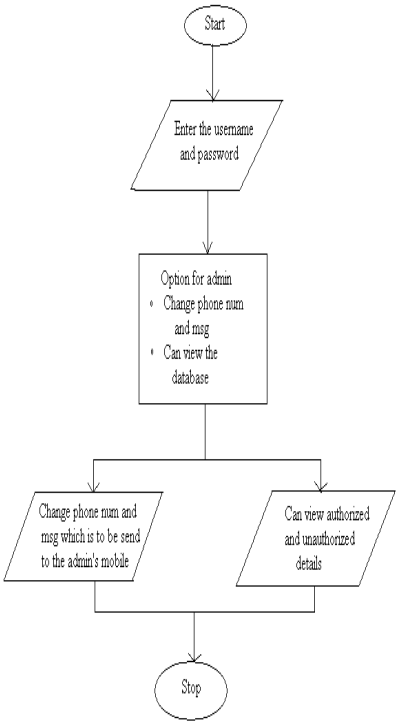

Fig 4.4 server login module

- **for client module:**

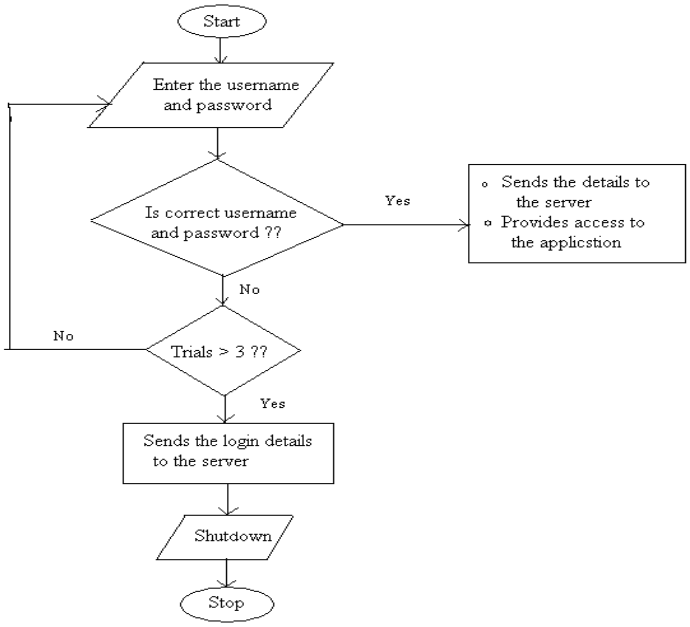

Fig 4.5 Client module

4.3 Snapshots

Server Login: The login snapshot in server side consists of text fields, labels and two buttons. The labels are "INTRUSION DETECTION SYSTEM ADMIN LOGIN", "Admin User ID", and "Admin Password".0The text fields for the entering the administrator's user id and administrator's password respectively. The button "Admin Login" used to authenticate login into the administrator details.

Fig 4.6 Server login page

Server Change Password: The snapshot for the changing the administrator password is shown below. The text fields provided here used enters the old username and password and can change the new password and new username. The button "change" is clicked inorder to change the user name and password.

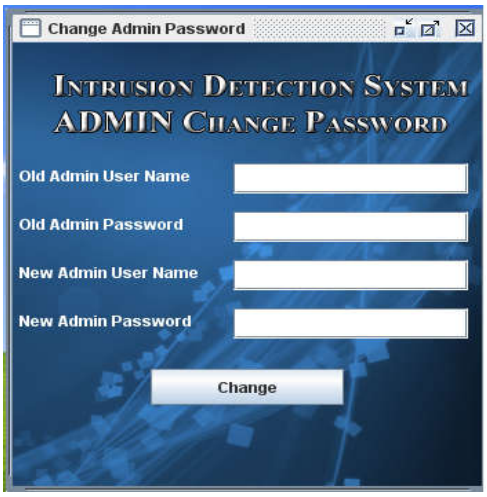

Fig 4.7 Password Change page

Server The proposed system welcome: The "the proposed system welcome admin**"** text is displayed in case of correct username and correct password. The button "Admin Details" is used in order to change the administrator mobile number and the message which is to be sent. The button "User Login Details" is used to view the details entered by the client systems.

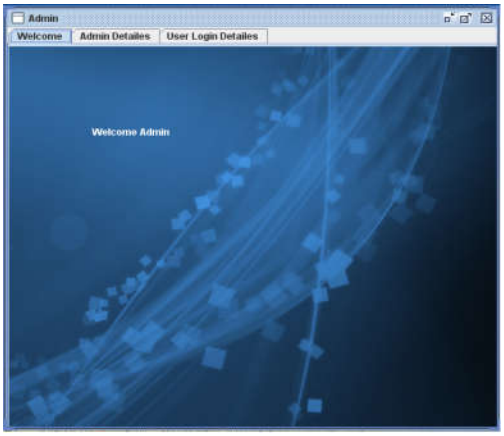

Fig 4.8 Server the proposed system welcome page

Server Detail: The snapshot below shows the administrator's details. The text fields are used to update the new administrator mobile number and the message which is to be sending to the administrator. The "Update" button is used to update the new phone number and message.

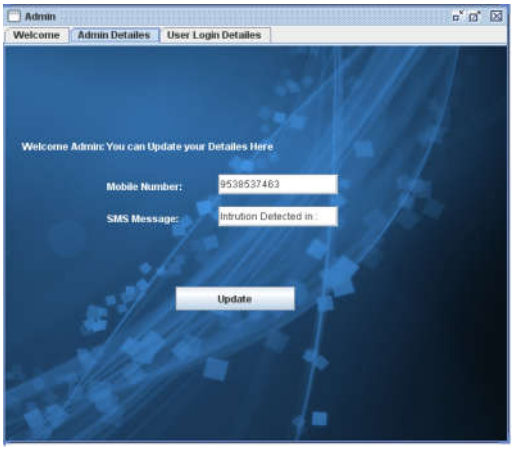

Fig 4.9 Server details page

User Login Visualization: The below shown snapshot shows the all the valid and invalid details entered in the client systems. The "IP Address" column shows the IP address of the particular system entered by the user. The "User" column shows the user name entered by the clients. The "Time" column indicates the time in which particular client has entered.

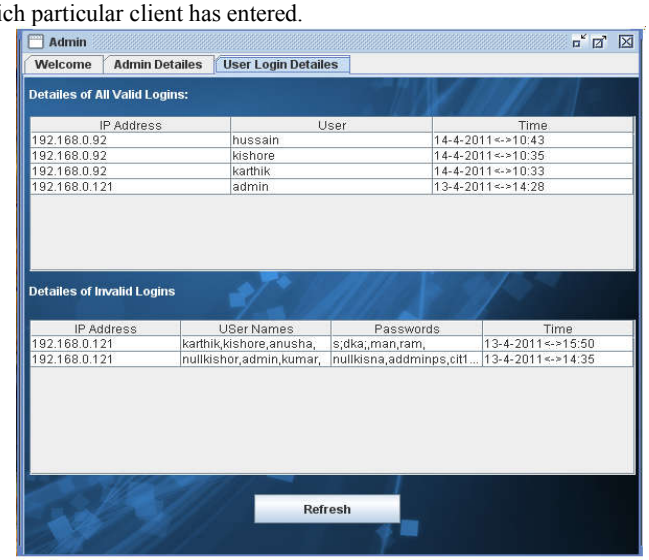

Fig 4.10 Database of user details

Client Login: The snapshot shown below is used to enter the username and password. It allows using the system in case of correct username and correcting password. The client has three attempts to validate himself in case of wrong password or wrong username.

Fig 4.11 Clients login page

V. Results

Test cases for client module login page:

Sl no	Test Case Input Description	Expected Result	Status
1	If the trails for the login to an application is <3	Display the login page again and again, to enter the correct user name and the password.	-
2	Correct user name and the correct password	Access to the application	pass
3	Correct user name and incorrect password	Display the login page again and again, to enter the correct user name and the password.	fail
4	Incorrect user name and correct password.	Display the login page again and again, to enter the correct user name and the password.	fail
5	Incorrect user name and incorrect password	Display the login page again and again, to enter the correct user name and the password.	fail
6	If the trails for the login to an application is >3	1. Send message to admin mobile, 2. store the details of username and the password in the database and 3. Shutdown the system.	-

Table 5.1 Test cases for client module login page

Test cases for server module:

Sl no	Test Case Input Description	Expected Result	Pass/ Fail
1	Correct admins username and the correct admins password	Access to the system and can look to the databases where users login details are stored.	pass
2	Correct user name and incorrect password	Display the login page again and again, to enter the correct admins user name and the password.	fail
3	Incorrect user name and correct password.	Display the login page again and again, to enter the correct admins user name and the password.	fail
4	Incorrect user name and incorrect password	Display the login page again and again, to enter the correct admins user name and the password.	fail

Table 5.2 Test cases for server module

VI. ADVANTAGES

Some of the advantages of our Intrusion Detection and Avoidance System are as follows:

- The particular system or application is allowed only if the user knows the correct user name and password. An intruder or attacker cannot use the secured system unless the correct login details are known.
- If unauthenticated person tries to access the client system, notification will be made to the system administrator mobile. A text message will be send.
- The administrator can view the login details entered by the user and can view the corresponding IP address of the client system
- Incase of unauthenticated access to login page, after number of trials the particular system gets automatically get shutdown.

VII. LIMITATIONS

Every system has some limitations, in our project also some of the limitations are described below:

- In order to send the text message to the administrator mobile usage of GSM modem is compulsory. GSM modem acts as the intermediate bettween administrator system and mobile.

- If the intruder knows the user name and password, he can access that particular system. Here the application fails to detect in case of known intruder.
- The proposed system is applicable only to LAN. For internet or WLAN this system is not applicable.

VIII. APPLICATIONS

The intrusion detection and avoidance system can be used in case of an office environment where sharing of system becomes necessary sometimes. In case of sharing the user must know the username and password of his/her system. If they try to hack others system the administrator will be notified and the system automatically get shutdown.

This has wide range of application even in the real time environment wherever authentication procedure is followed by using the password and username login form. One such area would be the ATM which that has two layer security of username and password. By adding this feature along with the capability of camera to take picture automatically and to store it in database would be helpful to detect the intruder who is trying for unauthorized access of account and withdrawal of money from that account could avoided. And also the account holder's cash is protected and he will be notified with SMS alert.

IX. CONCLUSION & FUTURE ENHACEMENTS

In the proposed system "Intrusion detection and avoidance system", the proposed system has enhanced the security for a common application running in PC's that are connected by a LAN. Here the proposed system has provided a controlled access to that application through the login form. In case an intruder tries to access the application with incorrect password and username then server will get notified after a specific number of trail and a notification message will be send to the administrator mobile through GSM modem. The PC through which the intruder had tried to access the application will be automatically gets shutdown as he finishes his available trials.

Hence the intruder will be avoided from accessing application once again after the specific number of trial. The server administrator will have the at most possible time of 2-5 minutes. Within that time administrator may be able to know the condition even if he is at the remote place away from the server. The only limitation that is to be considered is that the mobile phone number that he provided in the database should be valid. Mobile phone that he is carrying with him should be using the SIM which is having that same number and is to be under the network coverage. Once the Administrator knows the situation he may take action accordingly. So the application is protected from the unauthorized access.

FUTURE ENHACEMENTS

The proposed system can improve this application in the following ways:

- The proposed system can restrict the access of the user to certain public files on the PC only so that he/she cannot access administrator's private files.
- The proposed system can make the application to start automatically on system boot up and lock the PC so that power failure will not be a problem.
- The proposed system can take the image of the user who is using the system.
- Using Mobile the proposed system can visualize the database of the user details.

X. REFERENCES

Book reference

[1] The Complete Reference JAVA, Herbert Schildt, TATA McGRAW HILL, 7th edition.
[2] The Complete Reference J2EE, James Keogh, TATA McGRAW HILL, 1st edition.

Web reference

[1] http://download.oracle.com/javase/1.4.2/docs/api/javax/swing/package-summary.html
[2] http://download.oracle.com/javase/1.3/docs/api/java/awt/event/package- summary.html
[3] http://download.oracle.com/javase/1.4.2/docs/api/java/net/package-summary.html
[4]http://download.oracle.com/javase/1.3/docs/api/java/sql/package-summary.html
[4] http://en.wikipedia.org/wiki/Intrusion_detection_system
[5] http://modemsite.com/56k/x2-hyperterm.asp
[6] http://www.control.com.sg/at_commands_sms.aspx
[7] http://www.nowsms.com/faq/what-is-a-gsm-modem

BIOGRAPHIES

Chayashree G, Asst. Prof. GSSSIETW, Mysuru. Completed MTech in 2013 with Computer Science as a specialization in EPCET, Benagluru and Engineering in 2011 with Information Science as specialization. Got best paper award for "A Three Factor Authentication System Using Keystroke Dynamic" in NCRTCC-16. with a co author Jagadamba G Asst. Prof, Department of Information Science and Engineering ,SIT, Tumakuru,