Strategic Preincident Preparation With Geolocation For IT Forensics

Pradnya D. Nagare[1], Mayuri S. Kharjul[2], Chetana M. Patil[3] , Bhagyashri D. Kokate[4]

[1] *Department of Computer Engineering, Sandip Institute of Technology And Research Centre Nashik, Maharashtra, INDIA*
[2] *Department of Computer Engineering, Sandip Institute of Technology And Research Centre Nashik, Maharashtra, INDIA*
[3] *Department of Computer Engineering, Sandip Institute of Technology And Research Centre Nashik, Maharashtra, INDIA*
[4]*Department of Computer Engineering, Sandip Institute of Technology And Research Centre Nashik, Maharashtra, INDIA*

ABSTRACT

The strategy of a system being attacked by a anonymous entity is a common phenomenon now-a-days. The intensity of cyber attacks that are increasing day by day is able to influence a person physically, emotionally or mentally. The attacks sometimes may be single handed or it may be a collaborative aspect. The static distribution of IP addresses or the usage of information of by the internet service providers (ISP) which is responsible for the commitment of IP crime. After the commitment of such crime it is a tracability and recovery challenge for the department of IT Forensics. So, the current scenario follows the iterative based system development procedure using the geolocation for the perincident detection of attack with an increased probability of attack tracability. The system also follows the various techniques to provide security to the data of a particular registered user devices. Locating a particular attacker can be done using the georeputation in the geolocation technique. The proposed system focuses on the various security aspects to the data of the user.

Keyword: - *Georeputation, IP fluctuation, Geolocation, Preincident preparation.*

1. INTRODUCTION

The investigation of a attack after any incident is quite difficult for the current existing system to detect the attack in IT forensic. So this system deals with the problem of different attacks. On the system and its investigation using geolocation and preincidently strategic preparation approach for the security. The system mainly focus on the objectives of detection of attack on the system before the incident to be happened. Using the geolocation, the location of the attack is found by the technique of georeputation that is geolocational diamensioning. After investigation of attack, it can not be able recover the damaged files also it is very time consuming and it makes trouble for the user. To overcome all these problems we going to use preparation of strategy preincidently of an IT forensic using geolocation. Location of the attacker is described using geolocation. So doubtable connections are investigated deeply. georeputation technique helps to increase the traceability of attack and its recovery to the system. While accessing the data, this paper provides security to the data by providing the encryption and add exception of an extra IP address through which the user want to access the data. To detect the attack, IP address of that particular system was accomplished at the time of crime. Sometimes the information provided to the internet service provider can also be responsible for such kinds of attacks. So in such cases the reconstruction of the incident must be done. While reconstructing the path of the cyber crime such internet service provider, their related servers

and their clients needs to be investigated. Using the proposed system we can investigate for different security aspects for our data security.

2. DESIGN GOALS AND OBJECTIVE

1) To detect attack on the system preincidently.
2) To find exact location of the attacker using geolocation diamensioning.
3) To increase the traceability and recovery of the attack.
4) To provide security to the data by providing the encryption while accessing the data.
5) To maintain the log records of registered IP address that are distributed in the network while accessing the data via system.

3.DEFINITION OF TERMS

3.1Preincident preparation

The term strategic preincident preparation mainly refers to a planned action before happening of an incident which supports the activities of the investigation for the particular incident happened. These investigation activities may include the documentation of information, its previous and current existing records and the other related details.
The networking architectures, their log in details and history, the monitoring data in centralized located servers and their IT related applications such as the intrusion detection systems (IDS).

3.2Geolocation

The identification and geographical mapping of real world objects is known as geolocation. The practice assessing a new location with the refrence of previously assessed location can also be termed as geolocation. The locating engine uses the radio frequency (rf) locators such as Time Difference Of Arrival(TDOA) to find the location using mapping displays or other geographic information systems.
The geolocationing in computer techonology can be preformes by the association of the geographical parameters with the MAC address of the system, IP addresses, hardware production number or software embedded number, Wifi positioning system or device location co-ordinates. Geolocation automatically works after looking an IP address on WHOIS service and retrives the physical address of the registrant.

3.3Georeputation

The geolocation is the main concept of the system which is useful for the location detection of the attacker. But it is the crusial task due to the geographical proximity of the geographical areas. Georeputation follows the geographical proximity which is also called functional distance, which refers to the great extanent to location firms with an integration to the economic mechanisms and its social dimentions. The georeputation is related to the phenomenon that is currently spreading the increased innovation in the mobility of the individuals. The georeputation majorly reflects the concept of geological information with the consideration of geographical location detection. Previous to this creating an overview of the attack is the important task for using geolocation. Once the local identification of the attack is done, the origin of the data packet is detected the connection of the data comes into the picture. So now the reconstruction of the attack must be done for this the attack path is needed to be reconstructed to find the nearby affected systems in the centralized situated view of IP clusters. The discovery of the identity of the attack and the corresponding IP must be detected. It can be detected only when the ISP will be detected usually who is responsible at the time of attack.

3.4 IP Fluctuation

IP address is allocated to the system by internet service provider (ISP) using DHCP (Dynamic Host Control Protocol). So whenever system connects to internet ISP allocate a random unused IP address. If we are using private area network then we can allocate static IP address for each machine.

4. BASIC ARCHITECTURAL MODEL OF THE SYSTEM

Basic idea of publishing this paper is to create advance and optimal starting point on which forensic investigation will be based on "preincident".In this paper the concept of Wireless network is used for the interaction.

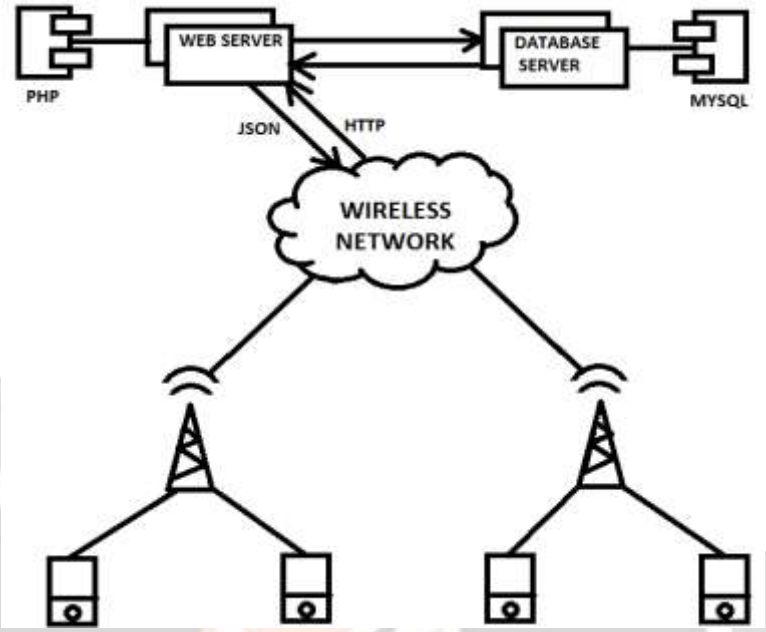

Fig -1: Architectural View

4.1 Wireless Network

Radio wave uses wireless local area network to connect devices such as android or laptop to the internet. Robust security protection and reduce cost of wiring are the main advantages of wireless network.

There are few arguments that this system uses wireless network:

I. Increased mobility and collaboration
II. Improved responsiveness
III. Better access to information
IV. Easier network expansion.

4.2 Server

The term database server is computer program. which provide databases services to computer. Database server holds the DBMS i.e. Database Management System and database. whenever is client sends a request the selected records are searched in database accordingly. For accessing, adding and managing the records or contents in database this system uses Mysql. Mysql is open source relational database management system i.e. RDBMS. Which is uses the SQL i.e. Structured Query Language. We are using Mysql for proposed system for quick processing, proven reliability, ease and flexibility of use. Web server uses HTTP (Hypertext Transfer Protocol) to serve files from web pages to user accordingly to their request. The proposed system uses the Hypertext Transfer Protocol. HTTP is an application protocol, which is foundation of data communication for the World Wide Web (WWW). We are using HTTP protocol for distributed collaborative and hypermedia information system. JSON (JavaScript Object Notation) for storing data and exchanging data, it is easier to use. It is easy for human to read and write as well as for machine to parse and generate.

5.SCENARIO

The basic scenario of this system deals with the development of the system with the above architecture along with the following flow of the system development lifecycle process. The process initiates the development of system with procedure of the identification and examination of the current existing system, their scenarios, used methodologies and their implementations. The existing system majorly focuses on the IP address of attack detection and its working is the same as that of an intrusion detection system(IDS).The new proposed system that is working on perincidently detection of the attack and its tracing based on the geolocation dimensioning. Geolocation is used to find the location of attacker and MAC address detection is used to detect the device used for the attack. The android devices are connected in a wireless network and the interaction between the web server and network takes place through the JASON and HTTP protocols. The front end of the system is designed using the android programming and backend is composed of MYSQL database server.

Now the developed system consist the various modules such as the user registration:

- user validation
- defining its geographical area through which he can access the data
- providing security encryption
- allowing user to add exception of MAC address
- maintaining the log in details of the user
- allowing the user to change the password whenever required

When the system is in the use the regular updation of user data, its geological location updation the user login details and password must be done for the well and secured functioning of the system.

The fig. 2 shows the different modules in the system and the architectural flow of the system.

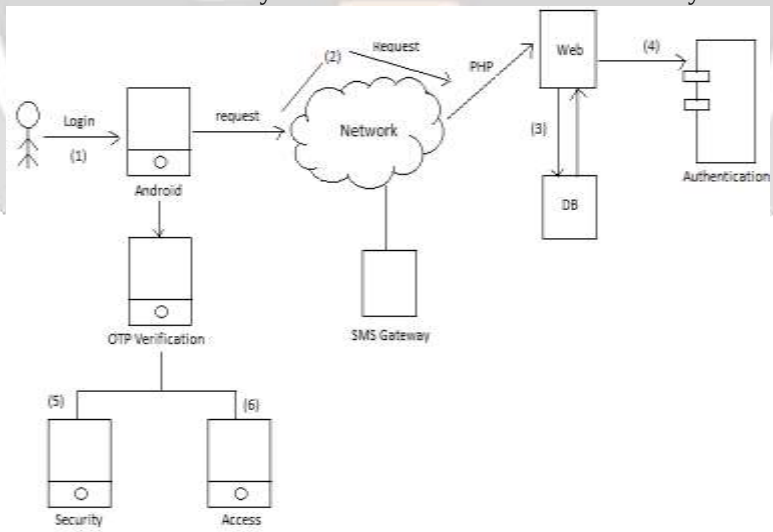

Fig -2:Architectural Flow of the system

5.1 Mathematical Model

The mathematical model of the system S can be written as:

S={U, I, P, D, O}

Where:

U= set of users
$\sum U_i$ = {U1, U2, U3,……, Un}
I = set of input
eg: Login details, Personel information, location etc.
P= set of processings
eg: Authentication, sms sending, etc.
D = set of devices
eg: Android devices, camera etc.
$\sum D_i$ = {D1, D2, D3, ……., Dn}
O = set of outputs
eg: login access/ denied, lock
open/closed, or camera locked or etc.

5.2Algorithm
"Secure Location Share and Distance Calculation Using SHA"

Algorithm steps:

1. Start
2. Read latitude and longitude of the system
3. Perform geocoding
4. Encrypt data using Secure Hash Algorithm
5. Get data record from database server
6. Calculate distance using formulas:
   Sin(deg2rad($lat1)) * sin(deg2rad($lat2)) +
   Cos(deg2rad($lat1)) * cos(deg2rad($lat2)) *
   Cos(deg2rad($theta))
7. Verify threshold
8. Perform action
9. Stop

The above algorithm gives the step by step working of the system . Reading the latitude and longitude of the the system is the initial step of the system that gives the dimensioning of the location of the system. After reading the dimensions of the location we perform the geocoding . The data in the database is encrypted by using the secure hash algorithm which uses the cryptographic hash function to provide security. The database server is responsible for the storage and maintenance of the data records, we access the records fron the database server of the system. To calculate the distance between recorded co-ordinates and current location we use the above formula for the disrance calculation. After the distance calculation we verify the threshold and perform the action accordingly. To define the more descriptive model, we use the use case diagram and uml diagram i.e fig. 3 and fig. 4.

5.3Usecase Diagram
The usecase diagram describes the user interaction with the system. While accessing the system the user gets registered to the system by providing the required information to the system. The system validates the user by providing the authorised username and password. After giving the authentication to the user the OTP (one time password) is provided to the user through sms and after the user enters the OTP to the system the user is validated. Then the geological authentication is done to find the geological dimensioning. The geological dimension includes the latitude and longitudinal parameters as the information to the system for distance calculation. Then the operations on the information are performed. After the registration of the usre profile the user is allowed to add the exceptions and manipulate the data or information. Then the user allowed to change the password if required.

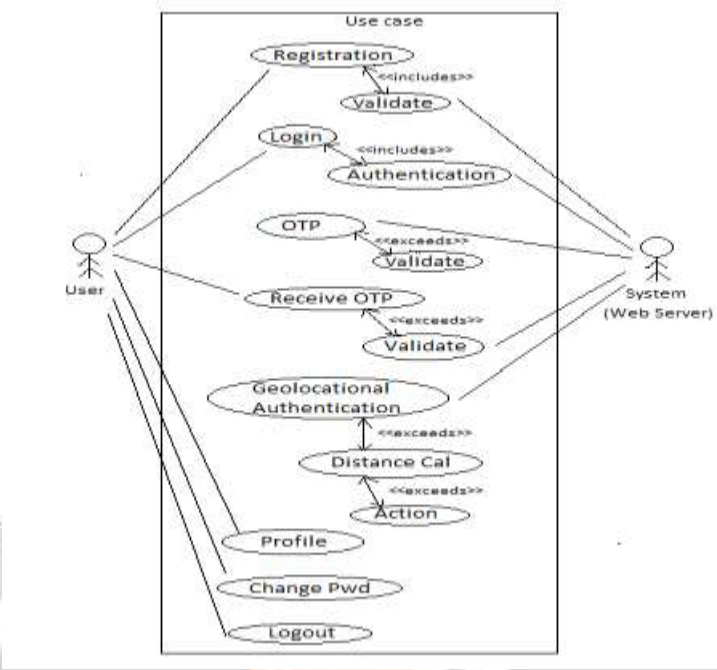

Fig -3: Usecase Diagram

5.4 UML Diagram

The UML diagram gives the relationship between the user, webserver and the database server. The user sends requests to the web server. The webserver is responsible for the validation of the user and providing the geological authentication to the validated user and the generation of the OTP and its distribution. All user information is recorded by the web server and stored in the database server. Everytime the updation of the newly entered data is carried out by the database server. The whole system provides the security and ease of access of data to the user.

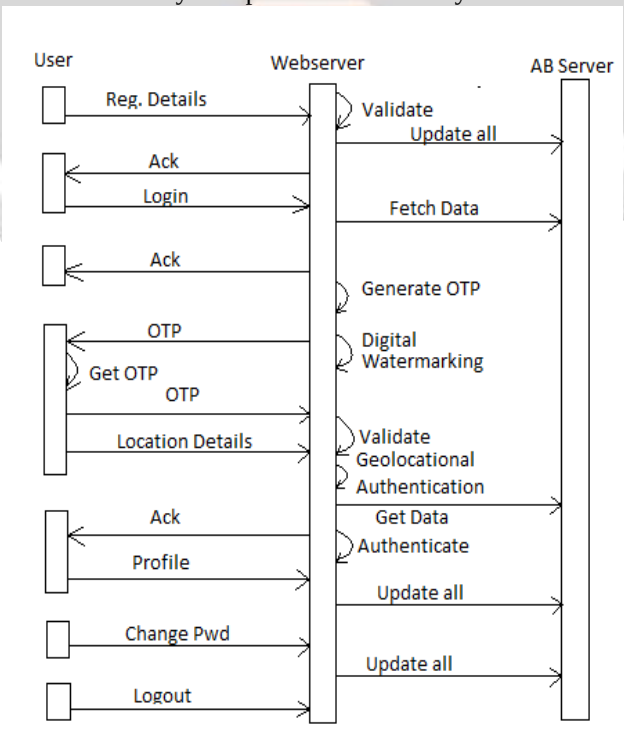

Fig -4: UML Diagram

6. CONCLUSION

The important phase of network foreignsic is preperation for strategic preincident. To support tracebility of attack and its attribution, optimal environment for subsequent investigation has to be created before the launching of attack. As this is mainly minimised to enabling capabilities of logging (such as activating MAC address based security and location based security and location based security on data). this paper suggest to use of MAC address based security to data, use of geolocation to detect the attack on the system preinsidently, to increase the tracability and recovery of the attack, to maintain the log record of IP address that are ditributed in network while accessing the data through the system. with the help of network forensic geo location provides i) detect the attack ii) location of attacker iii)security to data iv) to maintain the privacy of data of user or to avoid loss of important information of user

7. REFERENCES

[1].Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysi Robert Koch, Mario Golling, Lars Stiemert, and Gabi Dreo Rodosek IEEE SYSTEMS JOURNAL 1 2015.

[2]. A. Dahnert, "HawkEyes: An advanced IP Geolocation approach: IP Geolocation using semantic and measurement based techniques," in *Proc.2nd WCS*, 2011, pp. 1–3.

[3]. GEOGRAPHICAL PROXIMITY AND CIRCULATION OF KNOWLEDGE THROUGH INTER-FIRM COOPERATION *Delphine Gallaud and André Torre*

[4]. Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security Wanying Zhao, Gregory White The University of Texas at San Antonio

[5]. The Role of Geographical Proximity in Innova- tion Fraunhofer Institute for Systems and Innovation Research ISI Competence Center "Policy and Regions"

[6]. Traceability Challenge 2013: Statistical Analysis for Traceability Experiments Software Verification and Validation Research Laboratory (SVVRL) of the University ofKentucky Mark Hays, Jane Huffman Hayes Computer Science Department Arnold J. Stromberg, Arne C. Bathke Statistics Department University of Kentucky Lexington, Kentucky, USA mahays0@engr.uky.edu, hayes@cs.uky.edu